

# Shibboleth Training



Handouts

# Table of Contents

| Slide Set | Topic  | Page |
|-----------|--|------|
| 1.        | Federated Identity Management                  | 1    |
| 2.        | AAI Login Demo                                 | 11   |
| 3.        | Motivation for Using AAI                       | 19   |
| 4.        | SAML Terminology & Flows                       | 23   |
| 5.        | Introduction to Shibboleth                     | 29   |
| 6.        | Resource Registry                              | 35   |
| 7.        | AAI Attributes                                 | 38   |
| 8.        | Interfederation                                | 45   |
| 9.        | VHO & Swiss edu-ID                             | 50   |
| 10.       | SP Hands-On Session                            | 54   |
| 11.       | Try Demo Yourself                              | 110  |
| 12.       | X.509 Certificates for SAML                    | 111  |
| 13.       | Discovery Service Options                      | 114  |
| 14.       | Interfederation Attributes                     | 124  |
| 15.       | SWITCHtoolbox and Group Management Tool        | 128  |
| 16.       | SP Logout Support                              | 136  |
| 17.       | SP Virtualization                              | 144  |
| 18.       | SP Error Handling                              | 148  |
| 19.       | Shibboleth-aware Applications                  | 151  |
| 20.       | IdP Version 3 Upgrade                          | 155  |
| 21.       | IdP Configuration Pattern                      | 158  |
| 22.       | IdP User Authentication                        | 162  |
| 23.       | IdP Login Form Customization                   | 171  |
| 24.       | IdP Attribute Resolution                       | 180  |
| 25.       | IdP Persistent IDs                             | 190  |
| 26.       | IdP User Consent                               | 193  |
| 27.       | IdP Upgrades within Version 3                  | 206  |
| 28.       | IdP Updating the Home Organisation Description | 209  |
| 29.       | IdP Clustering                                 | 215  |
| 30.       | Resource Registry Interfederation Options      | 221  |
| 31.       | Entity Categories                              | 226  |
| 32.       | Attribute Release Configuration                | 231  |
| 33.       | IdP Overview of Log Files                      | 233  |
| 34.       | IdP Reloading the Configuration                | 238  |
| 35.       | New Challenges with Interfederation SPs?       | 241  |

# Federated Identity Management



# SWITCH

SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)

## Agenda

- What is Federated Identity Management?
- What is a Federation?
- The SWITCHaai Federation
- Interfederation

# Evolution of Identity Management

- Stone Age  
Application maintains unique credential and identity information for each user locally
- Bronze Age  
Credentials are centralized (e.g. Kerberos, LDAP) but applications maintain all user identity information
- Iron Age  
Credentials and core identity information is centralized and application maintains only app-specific user data

## Federated Identity

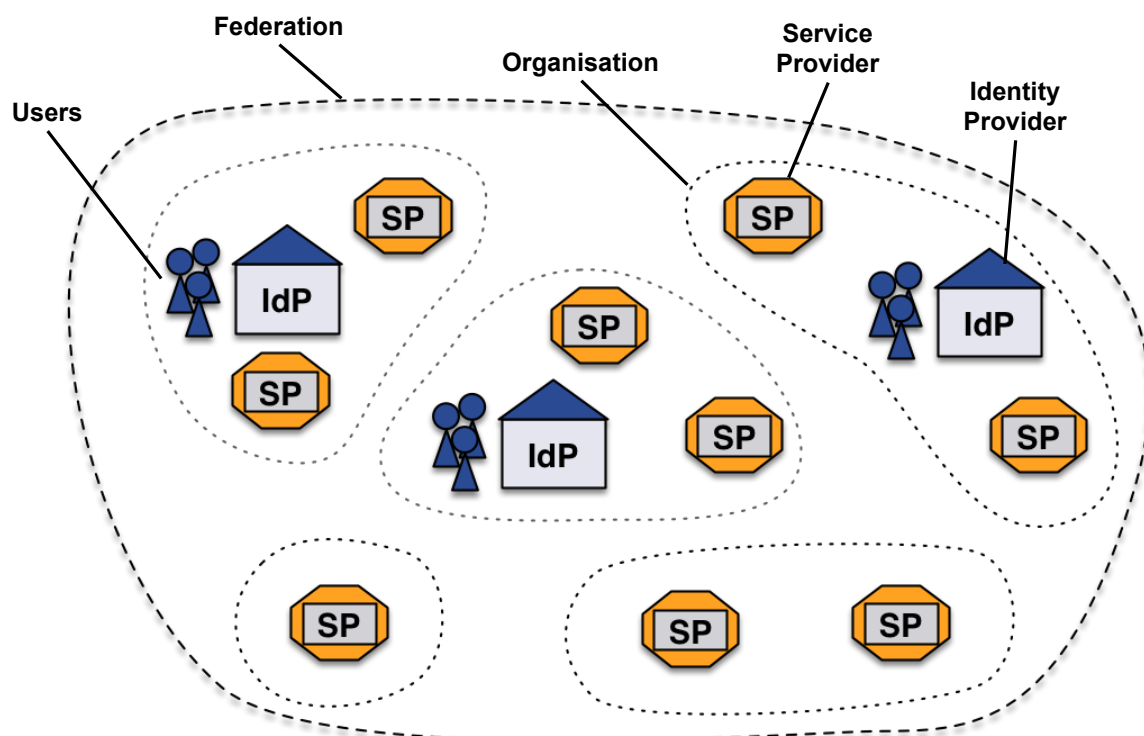
- Current mechanisms assume applications are within the same administrative domain
  - Adding an external user means creating an account in your IdM system. This could result in the new user having access to more than just the intended application.
- Federated Identity Management (FIM) securely shares information managed at a users home organization with remote services.
  - Within FIM systems it doesn't matter if the service is in your administrative domain or another. It's all handled the same.



# Federated Identity

- In Federated Identity Management:
  - **Authentication** (AuthN) takes place where the user is known
    - An **Identity Provider** (IdP) publishes authentication and identity information about its users
  - **Authorization** (AuthZ) happens on the service's side
    - A **Service Provider** (SP) relies on the AuthN at the IdP, consumes the information the IdP provided and makes it available to the application
  - An **entity** is a generic term for IdP or SP
- The first principle within federated identity management is the active protection of user information
  - Protect the user's credentials
    - only the IdP ever handles the credentials
  - Protect the user's personal data, including the identifier
    - a customized set of information gets released to each SP

## Federated Identity Management



# Benefits of Federated Identity Management

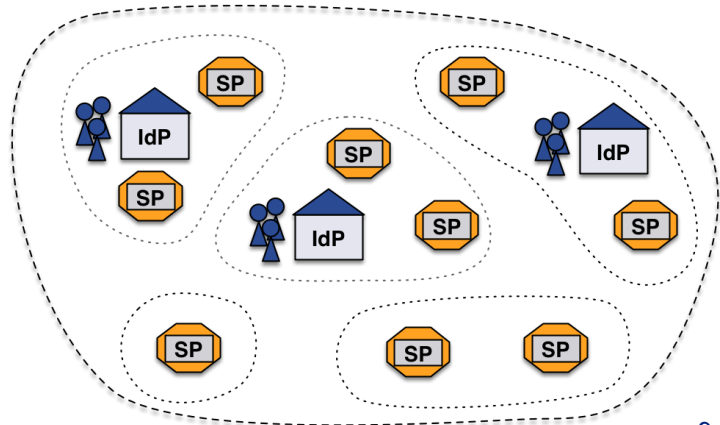
- Reduces work
  - Authentication-related calls to Penn State University's helpdesk dropped by 85% after they installed Shibboleth
- Provides current data
  - Studies of applications that maintain user data show that the majority of data is out of date. Are you "protecting" your app with stale data?
- Insulation from service compromises
  - With FIM data gets pushed to services as needed.  
An attacker can't get everyone's data on a compromised server.
- Minimize attack surface area
  - Only the IdP needs to be able to contact user data stores.  
All effort can be focused on securing this single connection instead of one (or more) connection per service.

## Some other gains

- Users generally find the resulting single sign-on experience to be nicer than logging in numerous times.
- Usability-focused individuals like that the authentication process is consistent regardless of the service accessed.
- A properly maintained federation drastically simplifies the process of integrating new services.

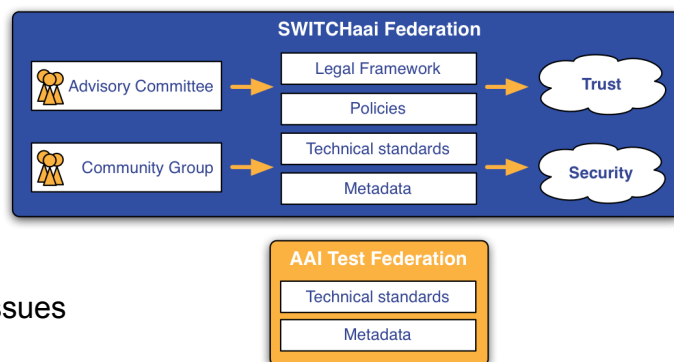
# What is a Federation?

- A group of organizations running IdPs and SPs that agree on a common set of rules and standards
  - It's a label - to talk about such a collection of organizations
  - An organization may belong to more than one federation at a time
- The grouping can be on a regional level (e.g. SWITCHaai) or on a smaller scale (e.g. large campus)
- **Note:**  
IdPs and SPs 'know' nothing about federations



## SWITCHaai (1)

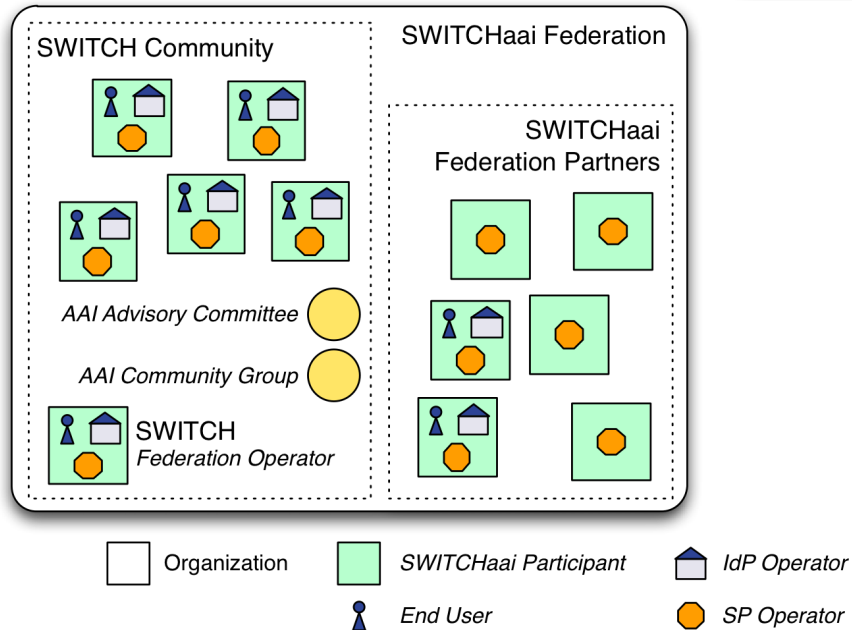
- SWITCH consults with two bodies
  - Advisory Committee deals with policies and legal framework
  - Community Group deals with technical/operational issues



- Two kinds of SWITCHaai Participants
  - **SWITCH Community**
    - Organisation fits the definition from the SWITCH Service Regulations
  - **SWITCHaai Federation Partner**
    - Organisation sponsored by a SWITCHaai Participant from the SWITCH Community

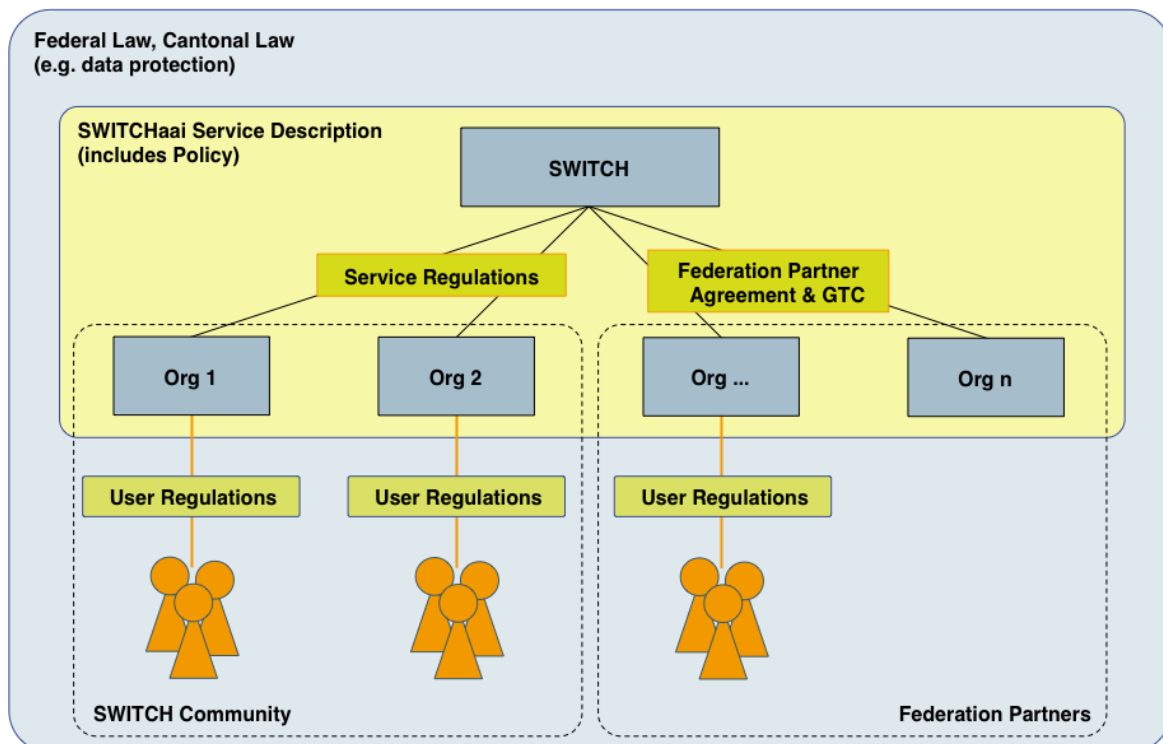
<https://www.switch.ch/aai/about/federation/>

## SWITCHaai (2)



- SWITCH operates the SWITCHaai Federation
- AAI is a Basic Service for the SWITCH Community

## SWITCHaai: The Legal Framework



# SWITCHaai: Rules, Policies, & Agreements

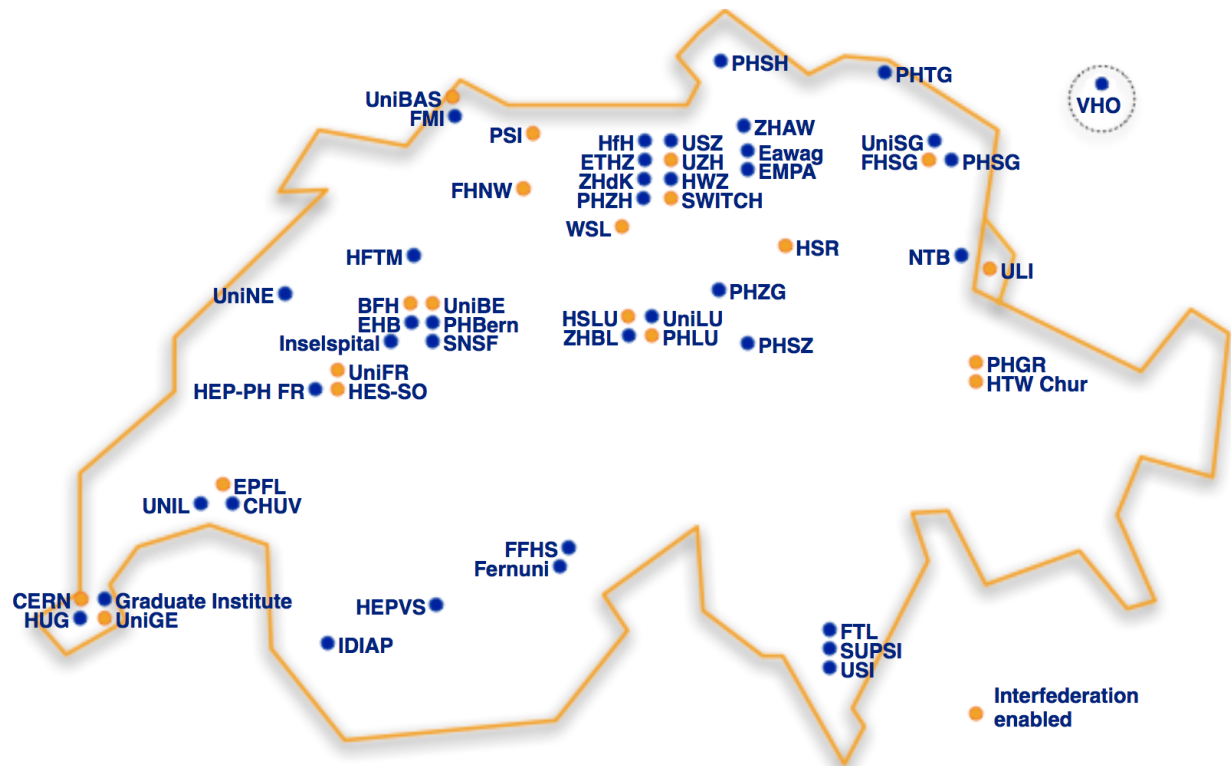
- **SWITCHaai Service Description** (includes the Policy)  
concepts and rules for all entities in the federation  
[https://www.switch.ch/aai/docs/SWITCHaai\\_Service\\_Description.pdf](https://www.switch.ch/aai/docs/SWITCHaai_Service_Description.pdf)
- **SWITCHaai Federation Partner Agreement**  
legal contract between SWITCH and federation partner
- **Certificate Acceptance Policy**  
policy certificates accepted by the federation  
<https://www.switch.ch/aai/support/certificates/certificate-acceptance/>
- **AAI Attribute Specification**  
minimum set of core and optional attributes supported  
by federation entities  
[https://www.switch.ch/aai/docs/AAI\\_Attr\\_Specs.pdf](https://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf)
- **Best Current Practices for SWITCHaai service operations**  
Common practices for operating an IdP or SP  
<https://www.switch.ch/aai/bcp>

## SWITCHaai: Services Provided

- Rules, policies and agreements  
<https://www.switch.ch/aai/documents>
- Guides: installation, configuration & migration  
<https://www.switch.ch/aai/guides>
- Centralized Services
  - Discovery Service  
<https://www.switch.ch/aai/tools>
  - Resource Registry, the federation management Web App
  - Virtual Home Organization (VHO)
  - Attribute Viewer & AAI Demo
  - Group Management Tool (GMT)
- Call-in helpdesk and email support: [aai@switch.ch](mailto:aai@switch.ch)
- AAI Test Federation
- Some application integration support
- Training



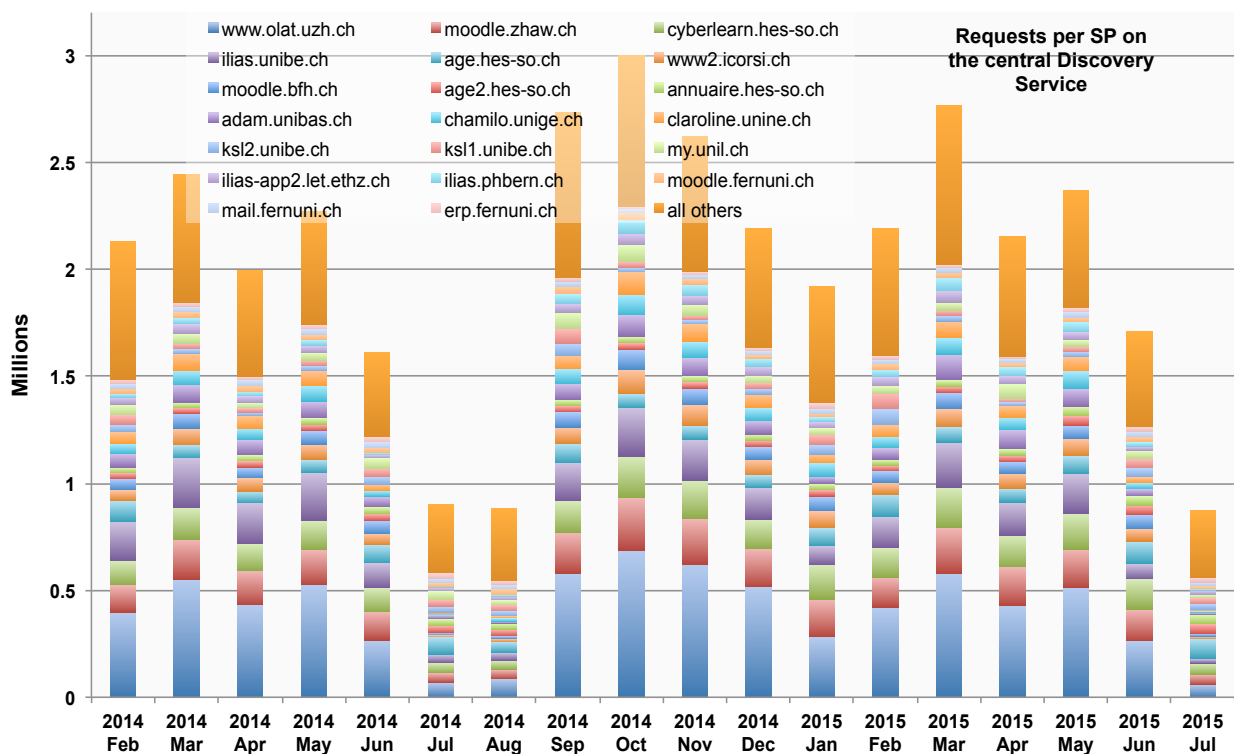
# SWITCHaai Federation Summer 2015



© 2015 SWITCH

17

## AAI User Authentication Requests Feb 14 – Jul 15

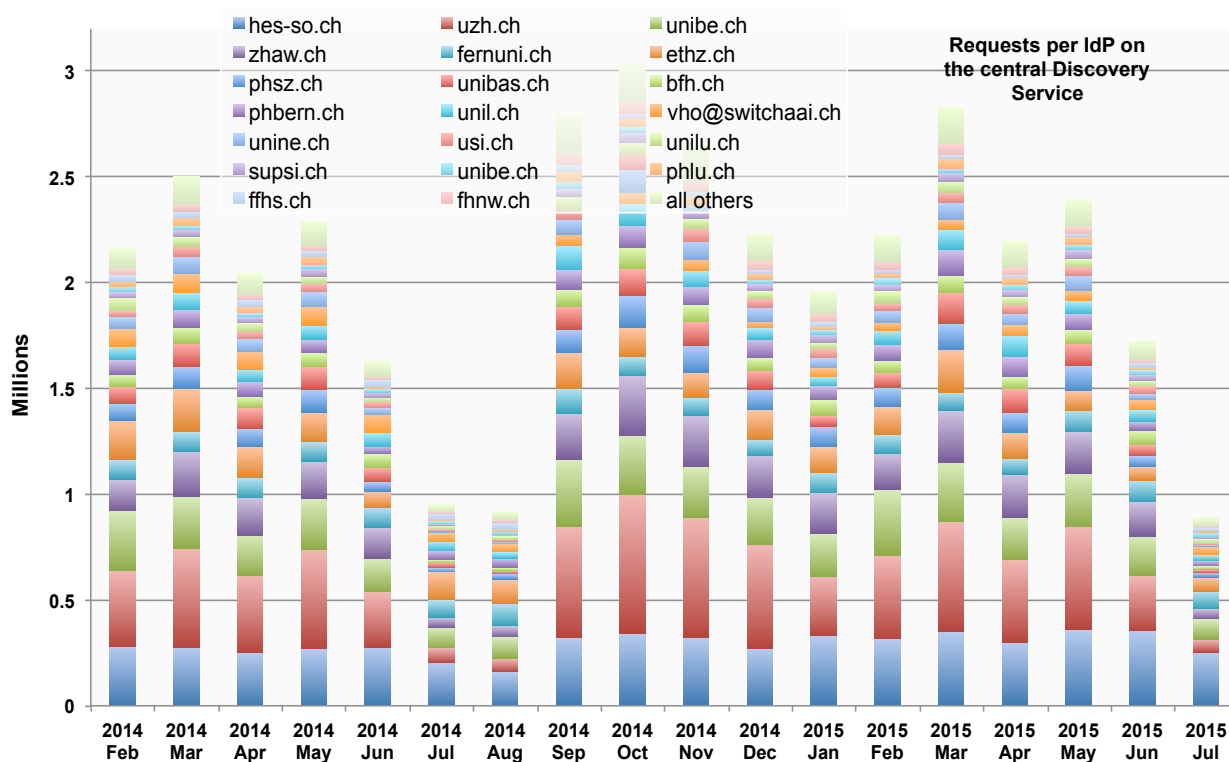


© 2015 SWITCH

AAI Discovery Service Stats – July 2015

18

## AAI User Authentication Requests Feb 14 – Jul 15



© 2015 SWITCH

AAI Discovery Service Stats – July 2015

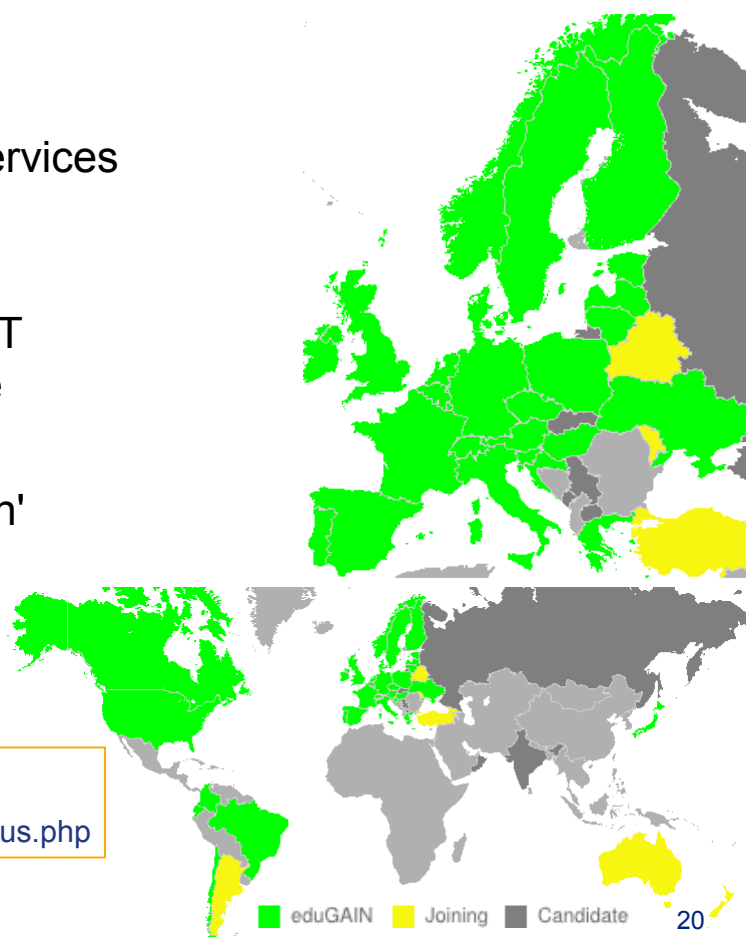
19

## Interfederation

- Users get access to services from other federations
- eduGAIN is the GÉANT Interfederation Service
- See the 'Interfederation' presentation.

<http://www.edugain.org>  
<https://technical.edugain.org/status.php>

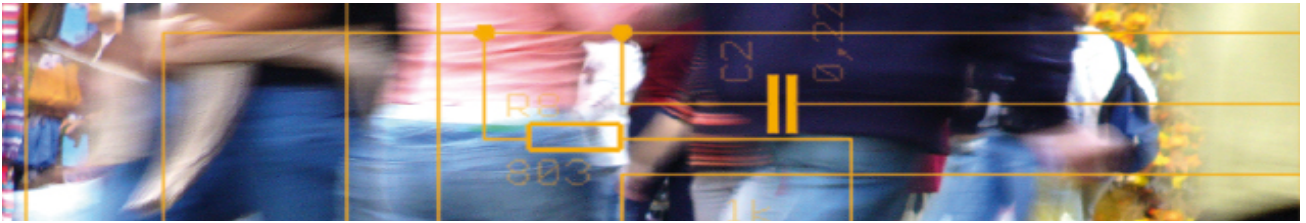
© 2015 SWITCH



20



# AAI Login Demo



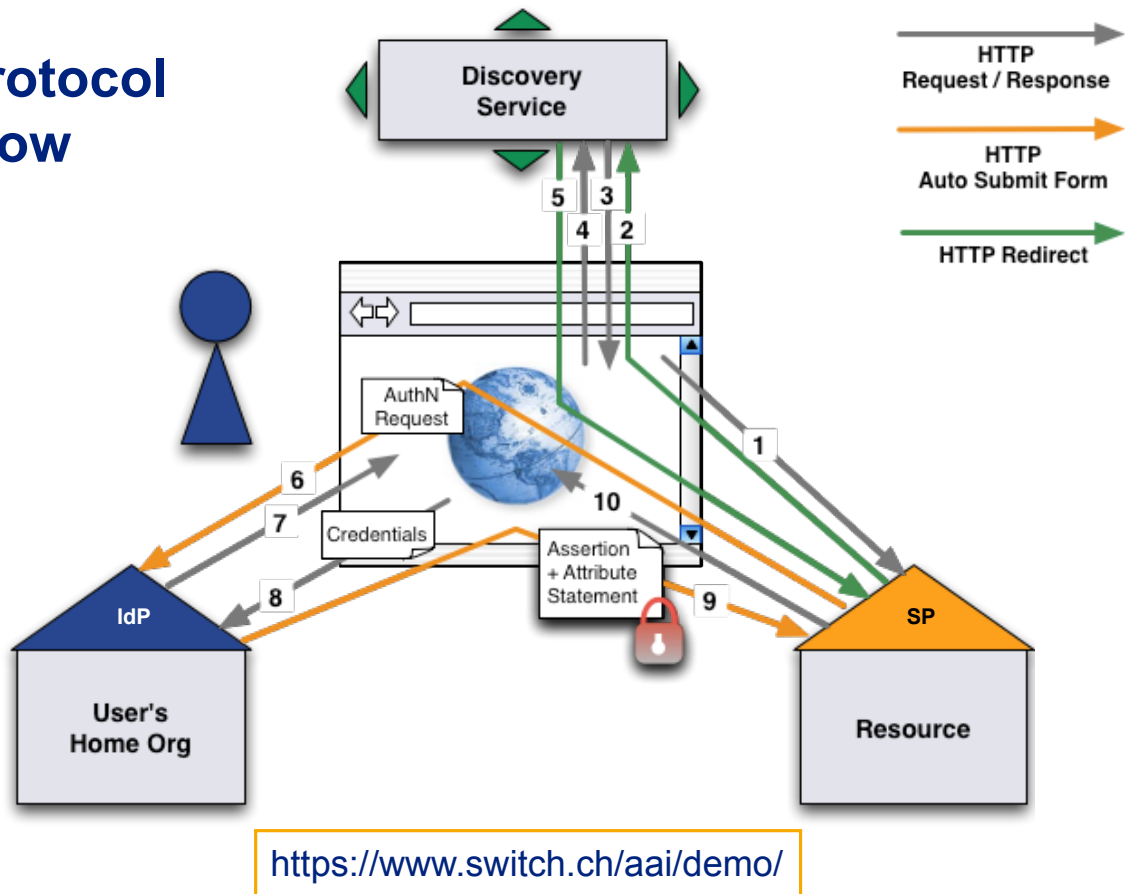
# SWITCH

SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)

## Agenda

- Illustration of protocol flow  
SAML2, Web Browser SSO
- Live demonstration

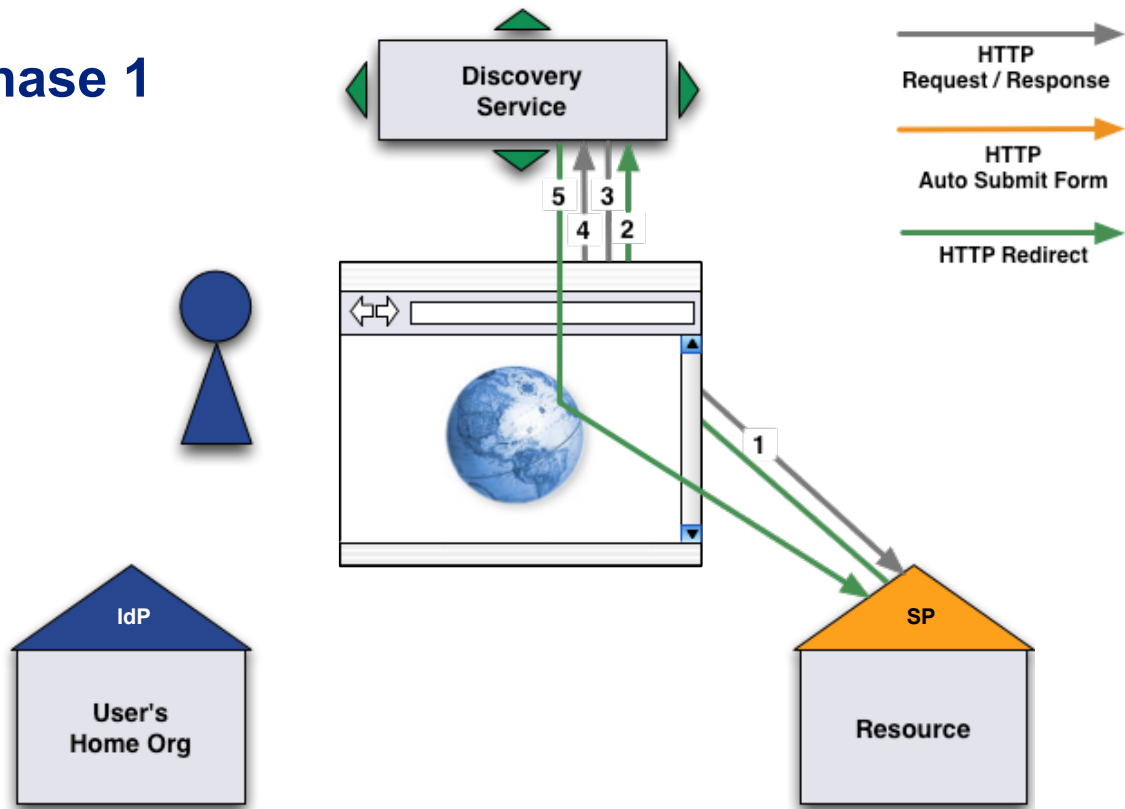
# Protocol Flow



## Phase 1

**First access to the Service Provider and Identity Provider discovery**

## Phase 1



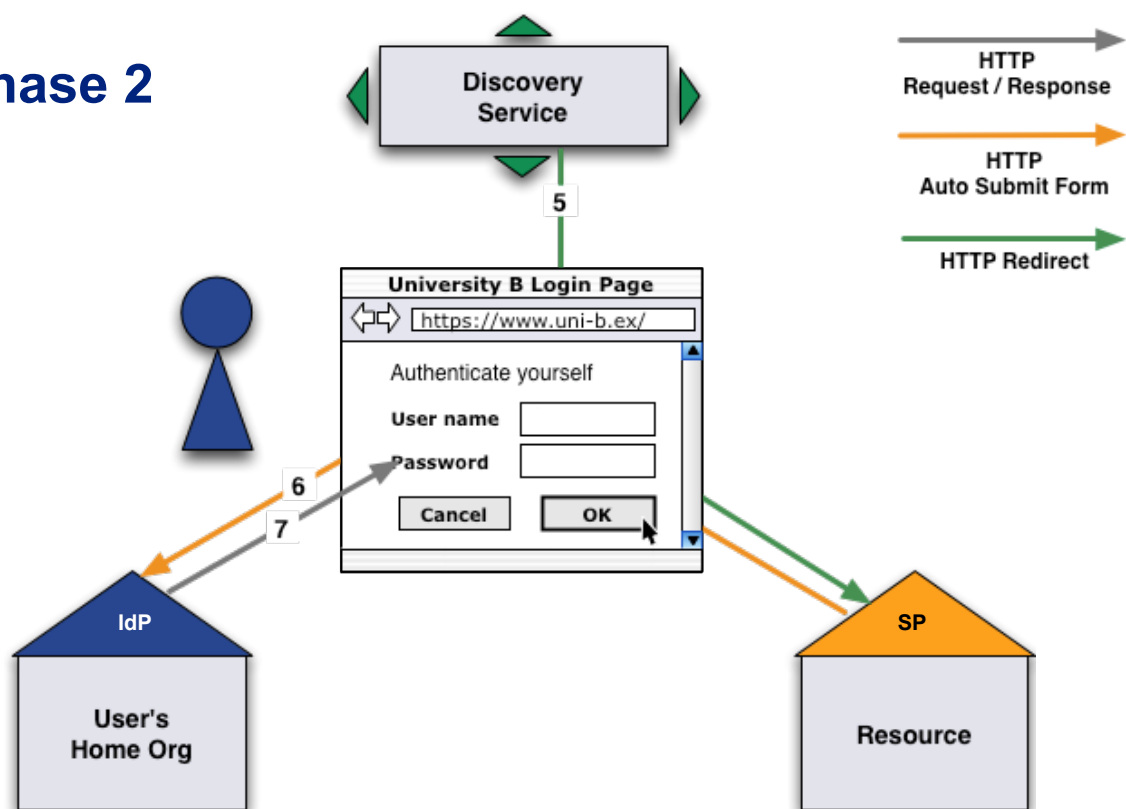
## First access to the Service Provider and Identity Provider discovery

- ① The user opens a web browser and accesses the Service Provider.
- ② The user is redirected to the Discovery Service by the Service Provider. Consequently, the web browser sends a new request to the Discovery Service.
- ③ The Discovery Service answers with the web page that allows the user to select an Identity Provider.
- ④ On the Discovery Service page, the user submits the Identity Provider selection.
- ⑤ The Discovery Service sends a redirect to the SP return destination, including the IdP selection.

## Phase 2

### Session initiation and authentication request

## Phase 2



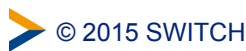
# SAML AuthN Request

Plain HTML:

```
<html>
  <body onload="document.forms[0].submit()">
    <form method="POST" action="https://aai-demo-idp.switch.ch/idp/profile/SAML2/POST/SSO">
      <input type="hidden" name="RelayState" value="ss:mem:23e3a3b1268acd89dc226bb1ce0d0c6ba7ecf773"/>
      <input type="hidden" name="SAMLRequest"
        value="PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1scD0idXJuOm9hc2lzOm5h...
        ...YXRlPSIxIi8+PC9zYW1scDpBdXRoblJlcXVlc3Q+"/>
    </form>
  </body>
</html>
```

SAML AuthN Request (Base64 decoded)

```
<saml:AuthnRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceIndex="1"
  Destination="https://aai-demo-idp.switch.ch/idp/profile/SAML2/POST/SSO"
  ID="_f2f27516ec08af29501c749629b119d3"
  IssueInstant="2008-02-27T12:17:40Z"
  Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    https://aai-demo.switch.ch/shibboleth
  </saml:Issuer>
  <saml:NameIDPolicy xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
    AllowCreate="1"/>
</saml:AuthnRequest>
```



9

## Session initiation and authentication request

- ⑤ The browser is redirected to the Service Provider by the Discovery Service.
- ⑥ The session initiator of the Service Provider creates an authentication request and returns it within an auto-submit-post-form to the browser.

The browser posts the SAML AuthN Request automatically to the Identity Provider using JavaScript.



10

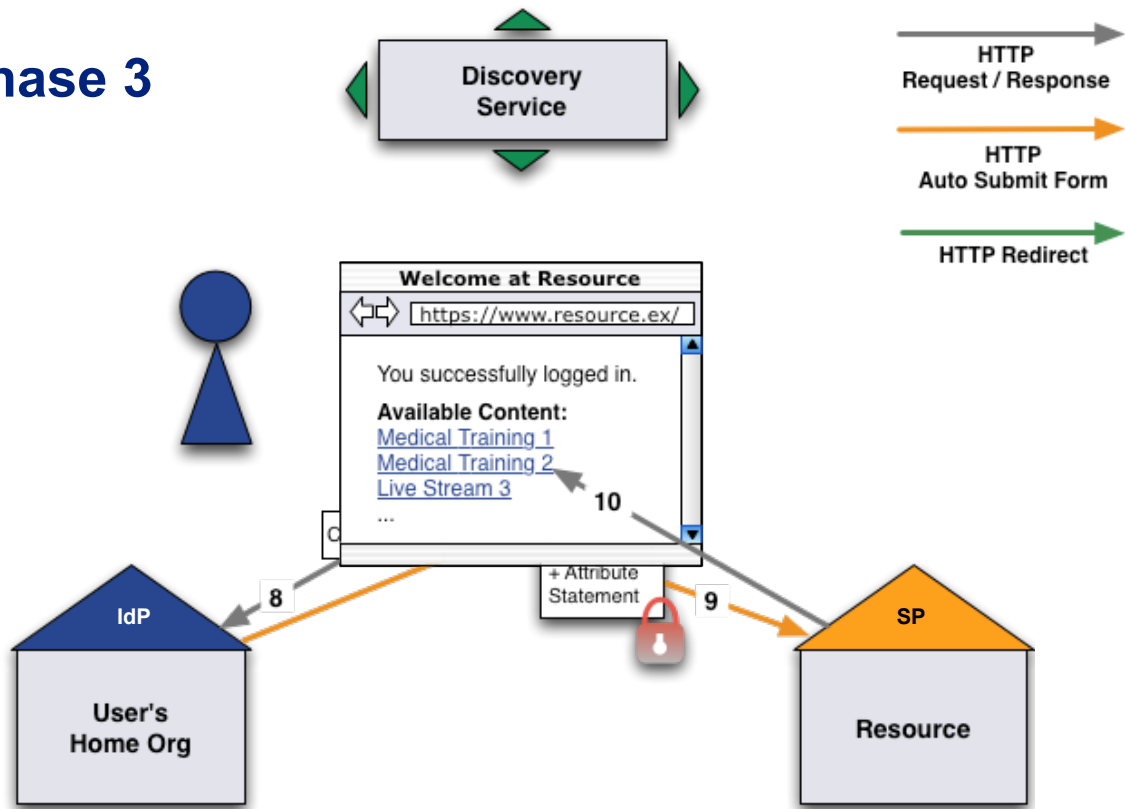
## Session initiation and authentication request

- ⑦ The Identity Provider checks the authentication request. Because the user hasn't yet been authenticated, the Identity Provider sends a redirect to the appropriate login page (usually: Username/Password).

## Phase 3

### Authentication, attribute statement and access

## Phase 3



## SAML Assertion + Attribute Statement

### Plain HTML

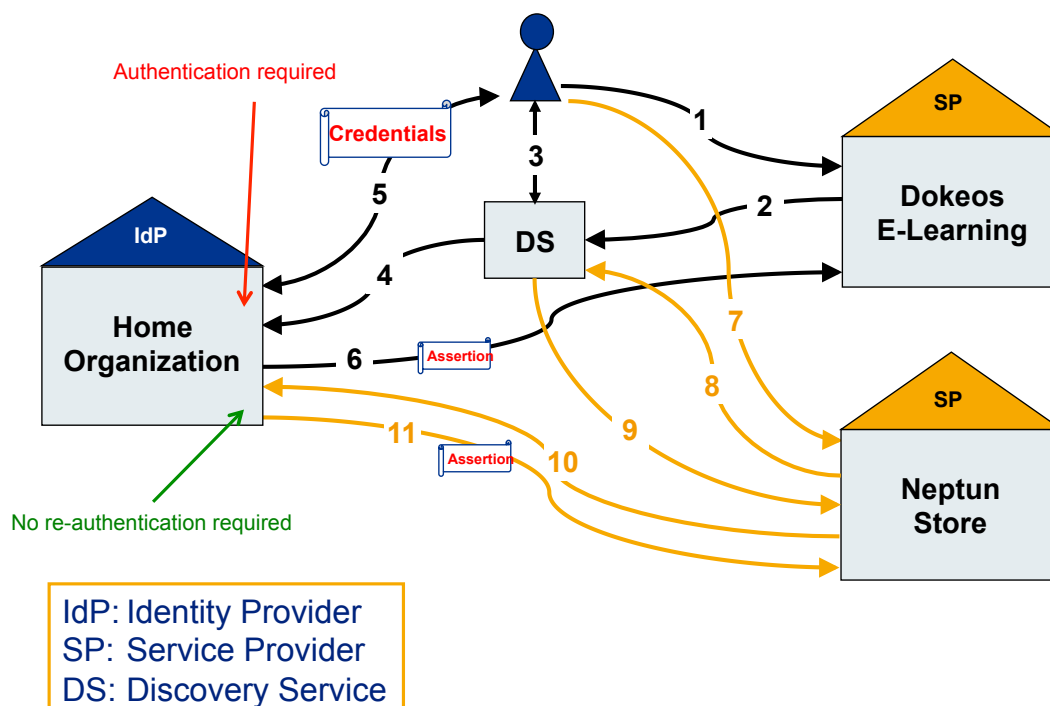
```
<html xml:lang="en">
  <body onload="document.forms[0].submit()">
    <form action="https://aai-demo.switch.ch/Shibboleth.sso/SAML2/POST" method="post">
      <div>
        <input type="hidden" name="RelayState" value="ss:mem:23e3a3b1268acd89dc226bb1ce0d0c6ba7ecf773"/>
        <input type="hidden" name="SAMLResponse"
          value="PD94bWwgdmVyc2lrbj0iMS4wIiB1bmNvZGluZz0iVVRGLTgiPz4KPHNhbnBwO8...
          ...vbj0iW1scDV1c+PC9zYW1scRGLsTgiPz4KP1c3U+"/>
      </div>
    </form>
  </body>
</html>
```

# SAML Assertion + Attribute Statement

SAML Assertion + Attribute Statement, decrypted (Base64 decoded)

```
<saml:Assertion ...>
  <saml:Issuer ...>
    https://aai-demo-idp.switch.ch/idp/shibboleth
  </saml:Issuer>
  <saml:Subject ...>
    <saml:NameID ...>
      _e7b68a04488f715cda642fbdd90099f5
    </saml:NameID>
    [...]
  </saml:Subject>
  [...]
  <saml:AuthnStatement ...
    AuthnInstant="2008-02-27T12:20:06.991Z"
    SessionIndex="4m2ETlKYtvbNEmBzVNo3UHLuKSdo3HqTUqAmeZiar94="
    SessionNotOnOrAfter="2008-02-27T12:50:06.991Z">
    [...]
  </saml:AuthnStatement>
  <saml:AttributeStatement ...>
    [...] (Attributes)
  </saml:AttributeStatement>
</saml:Assertion>
```

## Accessing multiple SPs





## Links

The AAI Demo shows how AAI works.

<https://www.switch.ch/aai/demo/>

The AAI Attribute Viewer shows which attributes are released by an Identity Provider.

<https://attribute-viewer.aai.switch.ch/>

# Motivation for Using AAI

From a web application developer's point of view



# SWITCH

SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)

# Why running AAI Services?

- Running a Service Provider requires some effort
  - Understanding non-trivial technology
  - Installing and configuring a SAML Service Provider (SP)
  - (Optionally) install and configure an IdP Discovery Service
  - (Optionally) adapt application or web server configuration
  - Keeping SP software up-to-date
- Why and for what reason do administrators of more than 830 AAI services and additional 960 eduGAIN services run SAML Service Providers?

## User Information in Form of Attributes!

Speaker's attributes on <https://av.aai.switch.ch>

| Attributes  | Values  |
|---|---|
| <b>persistent-id</b><br>SAML2 Attribute Name:<br>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent | <a href="https://aai-logon.switch.ch/idp/shibboleth!https://attribute-viewer.aai.switch.ch/shibboleth!yrVdvdAmohZY+cE6dcGvqu/Dubc=">https://aai-logon.switch.ch/idp/shibboleth!https://attribute-viewer.aai.switch.ch/shibboleth!yrVdvdAmohZY+cE6dcGvqu/Dubc=</a> |
| <b>uniqueID</b><br>SAML2 Attribute Name:<br>urn:oid:2.16.756.1.2.5.1.1.1                              | ██████@switch.ch  |
| <b>givenName</b><br>SAML2 Attribute Name:<br>urn:oid:2.5.4.42   | Lukas   |
| <b>surname</b><br>SAML2 Attribute Name:<br>urn:oid:2.5.4.4  | Hämmerle  |
| <b>mail</b><br>SAML2 Attribute Name:<br>urn:oid:0.9.2342.1.9200300.100.1.3                            | lukas.haemmerle@switch.ch   |
| <b>homeOrganization</b><br>SAML2 Attribute Name:<br>urn:oid:2.16.756.1.2.5.1.1.4                      | switch.ch   |
| <b>homeOrganizationType</b><br>SAML2 Attribute Name:<br>urn:oid:2.16.756.1.2.5.1.1.5                  | others  |
| <b>affiliation</b><br>SAML2 Attribute Name:<br>urn:oid:1.3.6.1.4.1.5923.1.1.1.1                       | <ul style="list-style-type: none"><li>• member</li><li>• staff</li></ul>  |
| <b>cn</b><br>SAML2 Attribute Name:<br>urn:oid:2.5.4.3   | Lukas Haemmerle   |
| <b>dateOfBirth</b><br>SAML2 Attribute Name:   | ██████  |

# Motivation for Running AAI Services

## ■ User Attributes

- Trusted and up-to-date information about user and his organisation
- Attributes are (typically) verified and set by organisations  
e.g. when student enrolls or when staff member is hired
- Self-interest of organisation to keep data up-to-date!

## ■ Attributes available to services outside organisation

- Easier collaboration/sharing of services

## ■ User has a single account/password

- Only one password needed to access AAI services
- Service in own organisation, SWITCHaai, world-wide via eduGAIN

# How Are Attributes Used?

## ■ User identification

Who is user?

## ■ Authorisation/Access Control

Is user allowed to access file or perform action?

# Use Attributes for Apache Access Control

```
# Force user to authenticate on protected-directory
<Location /protected-directory>
  AuthType shibboleth
  ShibCompatWith24 On
  ShibRequestSetting requireSession true
  Require shib-attr homeOrganizationType university uas
</Location>
```

Works also in .htaccess files that are processed dynamically.

# Use Attributes for Complex Access Control

```
# Complex Shibboleth access control rule
<Host name="sp.example.org">
  <Path name="/protected" authType="shibboleth" requireSession="true">
    <AccessControl>
      <AND>
        <OR>
          <Rule require="uniqueID">23c90324u@ethz.ch</Rule>
          <Rule require="affiliation">student</Rule>
        </OR>
        <OR>
          <Rule require="homeOrganization">ethz.ch</Rule>
          <Rule require="homeOrganization">uzh.ch</Rule>
        </OR>
      </AND>
    </AccessControl>
  </Path>
</Host>
```

Allow ETHZ and UZH students and another user identified by a unique identifier.

## Use Attributes in Application

**Just read attributes from web server environment and use them.**

- No library required
- Same place like REMOTE\_USER or REMOTE\_ADDR is read from.

// PHP Example

```
$AAIUser->setMail($_SERVER["mail"]);  
$AAIUser->setGivenName($_SERVER["givenName"]);  
$AAIUser->setSurname($_SERVER["surname"]);
```

// Java Example

```
request.getAttribute("uniqueID")  
request.getAttribute("homeOrganization")  
request.getAttribute("affiliation")
```

# SAML Terminology & Flows



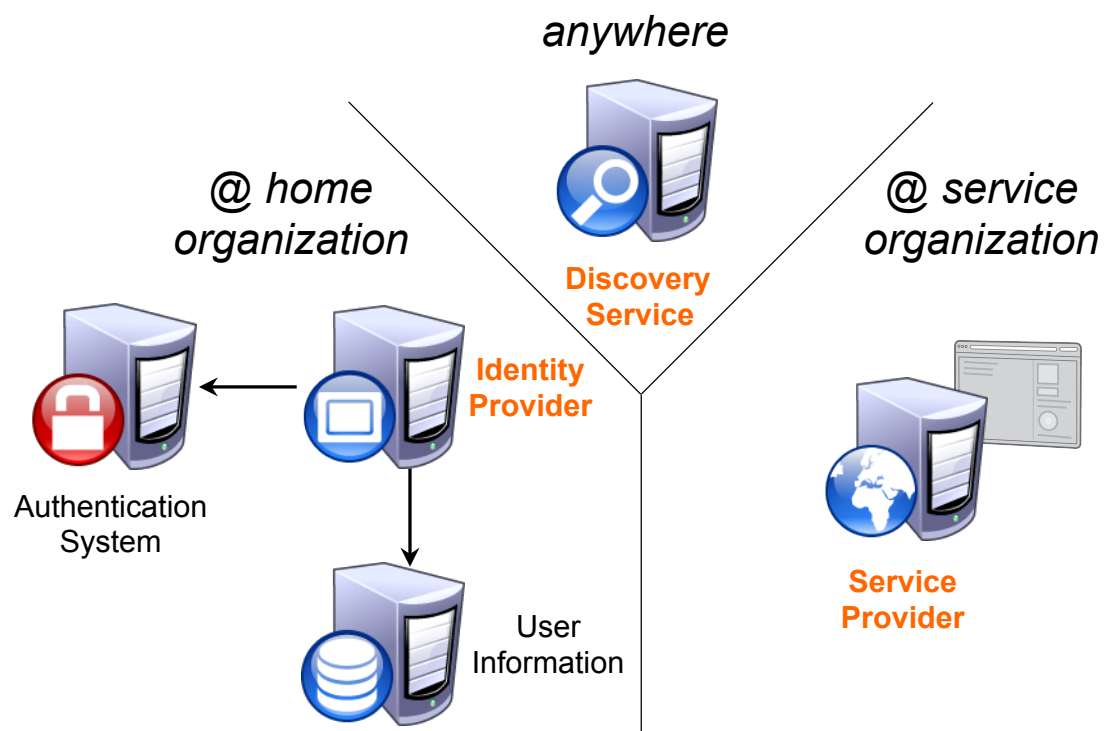
# SWITCH

SWITCHaai Team  
aai@switch.ch

# Agenda

- Components
- Terminology
- Communication Flow

## Components



## Components: Identity Provider (IdP)

- Authenticates users and provides information about users (attributes)
- Connects to **existing** authentication and user data systems
- Provides information about how a user has been authenticated
- Provides user identity information from the data source

## Components: Service Provider (SP)

- Component handling the SAML protocol and protecting the web application, typically running on the same server as the web application itself
- Initiates the request for authentication and attributes
- Processes incoming authentication and attribute information (SAML assertion from IdP)
- Optionally evaluates content access control rules
- Passes user information (attributes) to web application

## Components: Discovery Service (DS)

- Lets the user choose the home organization the user belongs to
- Tells the Service Provider which Identity Provider to use for authentication and attribute retrieval
- Can be integrated into the web resource or used as a separate central service
- Also known as "WAYF" (Where Are You From) service

## Terminology (1)

- SAML - Security Assertion Markup Language  
The OASIS standard describing the XML messages exchanged between IdP and SP (two versions: 1.1, 2.0)
- Profile - Standard describing how to use SAML messages to accomplish a specific task (e.g. SSO, attribute query)
- Binding - Standard that describes how to take a profile message and send it over a specific transport (e.g. HTTP)



## Terminology (2)

- entityID - Unique identifier for an IdP or SP

Examples:

- IdP: `https://aai-login.example.org/idp/shibboleth`
- SP: `https://moodle.example.org/shibboleth`

- NameID - An identifier by which an IdP knows a user

Examples:

- `234567@example.org`
- `https://aai-login.example.org/idp/shibboleth!` ↵  
`https://moodle.example.org/shibboleth!` ↵  
`d1FC71fyChS8kGdgYcacD3uoDOQ=`
- `_e7b68a04488f715cda642fbdd90099f5`

## Terminology (3)

- Attribute - A named piece of information about a user

Examples:

- givenName: John
- surname: Doe
- homeOrganization: example.org

- Assertion - The unit of information in SAML

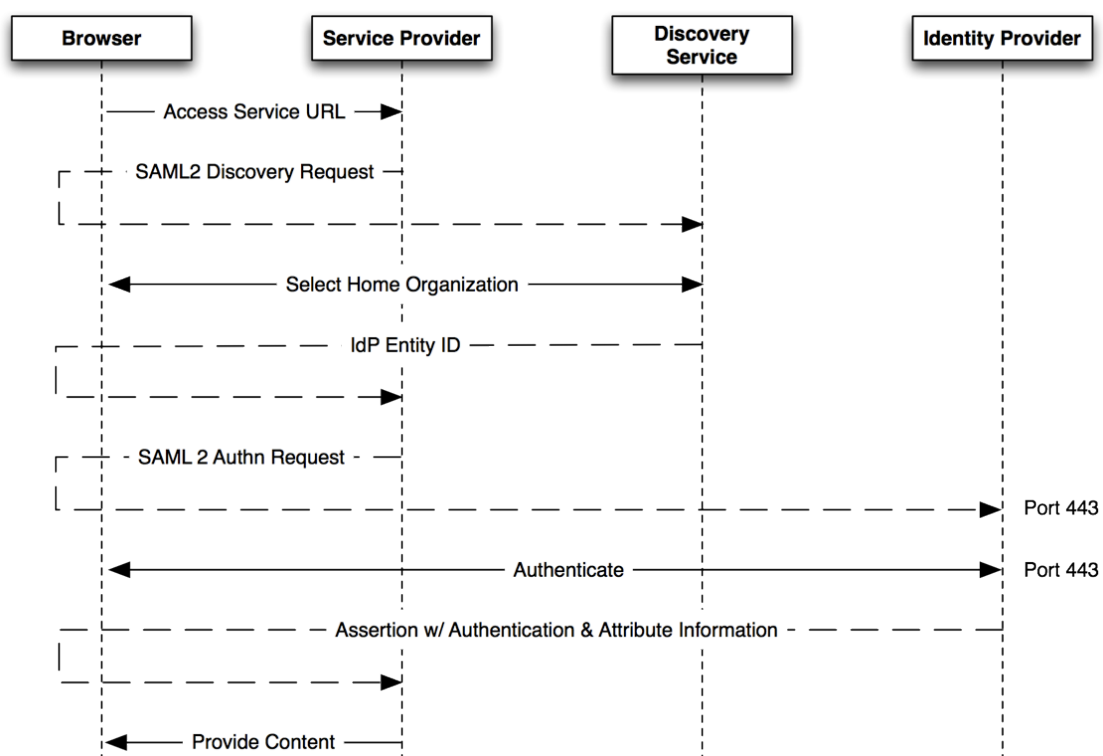
Example:

```
<saml:Assertion ...>
  <saml:Issuer ...>https://aai-login.example.org/idp/shibboleth</saml:Issuer>
  <saml:Subject ...><saml:NameID ...>_e7b68a04488f715cda642fbdd90099f</saml:NameID>
  </saml:Subject>
  <saml:AuthnStatement ... > ... </saml:AuthnStatement>
  <saml:AttributeStatement ...>
    [...] (Attributes)
  </saml:AttributeStatement>
</saml:Assertion>
```

## Terminology (4)

- Service / Resource  
Application that supports SAML  
(e. g. Moodle, Ilias, etc.)
- Service Provider: SAML component running on the application's server providing SAML support for the application
- "Shibbolized" application  
Application whose access is protected by SAML/Shibboleth

## Communication Flow: SAML 2 SSO



# Introduction to Shibboleth



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Agenda

- What is Shibboleth?
- Components
- Supported Profiles and Protocols
- Shibboleth in the Federation
- Support Resources

## Shibboleth – Origin and Consortium

- The Origin
  - Internet2 in the US launched the open source project in 2000
- The name
  - Word **Shibboleth** was used to identify members of a group
- The standard
  - Based on Security Assertion Markup Language (SAML)
- The Consortium
  - The new home for Shibboleth development
  - Collect financial contributions from deployers worldwide



<http://shibboleth.net>

## What is Shibboleth? (1)

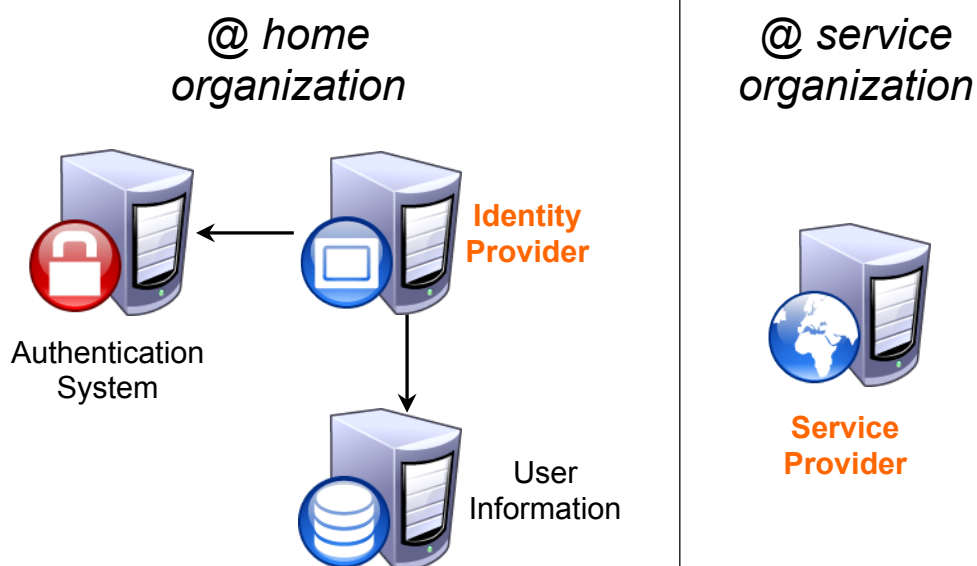
- Technically it's a project group, like Apache or Eclipse, whose core team maintains a set of software components
- Most people think of it as the set of software components
  - OpenSAML C++ and Java libraries
  - Shibboleth Identity Provider (IdP)
  - Shibboleth Service Provider (SP)
  - Shibboleth Discovery Service (DS)
  - Shibboleth Metadata Aggregator (MA)
- Taken together these components make up a federated identity management (FIM) platform.
- You might also think of Shibboleth as a multi-protocol platform that enforces a consistent set of policies.



## What is Shibboleth? (2)

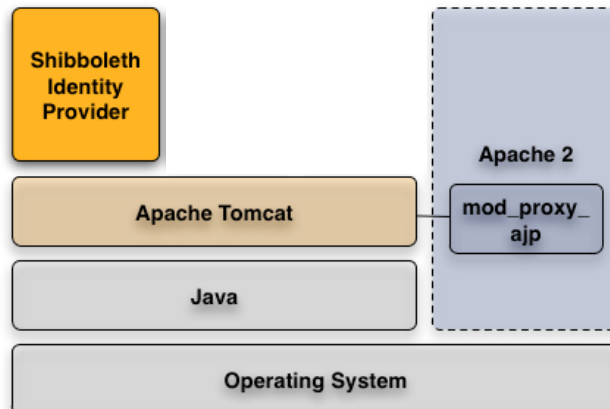
- The Shibboleth software components are an implementation of the SAML protocols and bindings. There are other products, too (like e.g. SimpleSAMLphp, ADFS).
- The Shibboleth software is widely used in the research and education environment

## Components used in the SWITCHaai federation



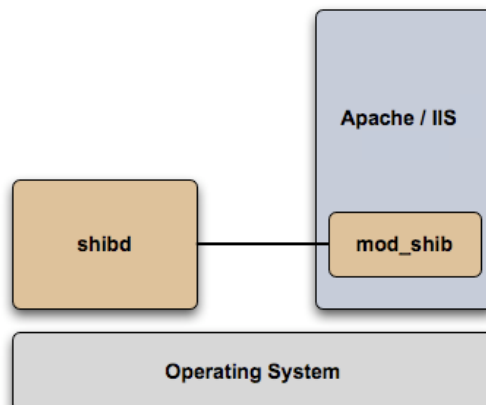
## Shibboleth Components: Identity Provider (IdP)

- What is it?
  - A Java Servlet web application
- What does it do?
  - Connects to **existing** authentication and user data systems
  - Provides information about how a user has been authenticated
  - Provides user identity information from the data source



## Shibboleth Components: Service Provider (SP)

- What is it?
  - mod\_shib: A C++ web server (Apache/IIS) module
  - shibd: A C++ daemon - keeps state when web server processes die
- What does it do?
  - Typically initiates the request for authentication and attributes
  - Processes incoming authentication and attribute information
  - Optionally evaluates content access control rules



## Shibboleth Components: Others

Further Shibboleth components:

- Shibboleth Discovery Service (DS)
  - Not used in SWITCHaai
  - Instead, we use the SWITCHaai WAYF
- Shibboleth Metadata Aggregator (MA)
  - Used in the Resource Registry to support Interfederation resources

## Shibboleth Supported Profiles and Protocols

- SAML 2.0
  - **SSO**
  - Attribute Query
  - Artifact Resolution
  - Enhanced Client
  - Single Logout (SP-only)
- SAML 1.1 (deprecated)
  - SSO Profile
  - Shibboleth SSO Request Profile
  - Attribute Query
  - Artifact Resolution
- Discovery
  - **SAML 2 Discovery Service Protocol**
  - Shibboleth 1 Discovery (WAYF) Protocol

<https://wiki.shibboleth.net/confluence/display/DEV/Supported+Protocols>

## Shibboleth in the Federation

- Shibboleth knows nothing about federations, it just consumes metadata in order to:
  - Locate the entity to which messages are sent
  - Determine what protocols the entity supports
  - Determine what signing/encryption keys to use
- The “Resource Registry”, a central registry in the SWITCHaai federation, generates the metadata and makes all IdPs and SPs know each other
  - The Resource Registry knows all IdPs, SPs, supported protocols, service locations and signing/encryption keys

## Support Resources

- First, check with your Federation
  - <http://switch.ch/aai/support/documents>
  - <http://switch.ch/aai/support/help>
- Shibboleth Wiki
  - <https://wiki.shibboleth.net/confluence/display/SHIB2>
  - <https://wiki.shibboleth.net/confluence/display/IDP30>
- Shibboleth Mailing Lists
  - Available lists: <http://shibboleth.net/community/lists.html>
    - Users
    - Announcements
    - Development
  - User's list archive: <http://marc.info/?l=shibboleth-users>



# Resource Registry

How to manage Federation metadata and other descriptions



# SWITCH

SWITCHaai Team

aai@switch.ch

## The Initial <Problem>

```
</EntityDescriptor>
<!-- Resource Registry -->
- <EntityDescriptor entityID="https://rr.aai.switch.ch/shibboleth">
- <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:SAML:1.1:protocol">
- <Extensions>
- <mdui:UIInfo>
- <mdui:DisplayName xml:lang="en">Resource Registry</mdui:DisplayName>
- <mdui:Description xml:lang="en">
The Resource Registry is a tool developed by SWITCH collecting information about Resources and Home Organizations which participate in the SWITCHaai and AAI
</mdui:Description>
- <mdui:Keywords xml:lang="en">resources aai register authority administration</mdui:Keywords>
</mdui:UIInfo>
</Extensions>
- <KeyDescriptor>
- <ds:KeyInfo>
- <ds:X509Data>
- <ds:X509Certificate>
MIIDHDCCAgSgAwIBAgIJAKyuqWEMkbhhMA0GCSqGSIb3DQEBAQUAMBSxGTAXBgNV BAMTEHJyLmFhaS5zd2l0Y2guY2Y2gWHEcNMTEExMjA1MDczM/
MTE3WjAbMRkwFwYDVQQDExByci5hYWkuc3dpdGNoLmNoMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0BdooNoOCQhs4cHgPuKMi2
jfgYXkiHUD4mkHFWE4CqQVSfPcGbLLCj3Kb9O2a34F79mAJL3VIOUgc3MB4k74 vqqVuql5zLgjbzMZgXeG2pKtBQCiiEc0j/34EFFFTPXOG7MWEi8Nd5-
vU47u3BzOzxLhtMtZcfQonkmgFdm5IboE7Ltf5hoaqu/PP5YAPD5fQgLP59FgGT HJ673DDhHlmkpp17Yd4vGhi/zuuWwayqqrQ7McUw2IjJfQsXndZhSubOibL
sbHy/bTmltTQ1dHERhQnfl4PWOCw3oc4TVQv9TctksjTwIDAQABo2MwYTBABgNV HREEOTA3ghByci5hYWkuc3dpdGNoLmNoiNodHRwcovL3JyLmFhaS5-
Y2gvc2hpYmJvbGV0aDAdBgNVHQ4EFgQUbXFxLXgSki1u88YLDYREjH8f14wDQYJ KoZlhvceNAQEFBQADggEBAlpxIxpUReUSJkK6xcWXcjsUf1mU-
j5gmloJJB0dl1eEMWjoHrhelAFRKnjOx6+HentP7xWsV2mUAWTH9misPA6qZ0MZ AbW578ed1pZx04iqsZhAfFC8uh+GgCCnmX15f8W5LoDN+RDKIZfpodS-
yL1TAZIVVIH+HfmV1qut4u9HjqF3WUJ9hVP15IgjRoh9LbPrSOubJqO69mu4QDcA gv6tFqjiavGvM4p7EMZbcXQMtCajZz5SHSLXSGDNLKX+HePKvkSyk0CO
nhE8VWTzYa85XDuG2QBdczmVAKDom9zZcSMXMTxwmOs=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://aai-rr.switch.ch/aaitest/Shibboleth.sso/SLO/Redirect"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://rr.aai.switch.ch/aaitest/Shibboleth.sso/SLO/Redirect"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://rr.aai.switch.ch/Shibboleth.sso/SLO/Redirect"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aai-rr.switch.ch/aaitest/Shibboleth.sso/SLO/POST"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://rr.aai.switch.ch/aaitest/Shibboleth.sso/SLO/POST"/>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://rr.aai.switch.ch/Shibboleth.sso/SLO/POST"/>
```

Shibboleth needs SAML 2 metadata to know all entities!

## Difficulties and Goals

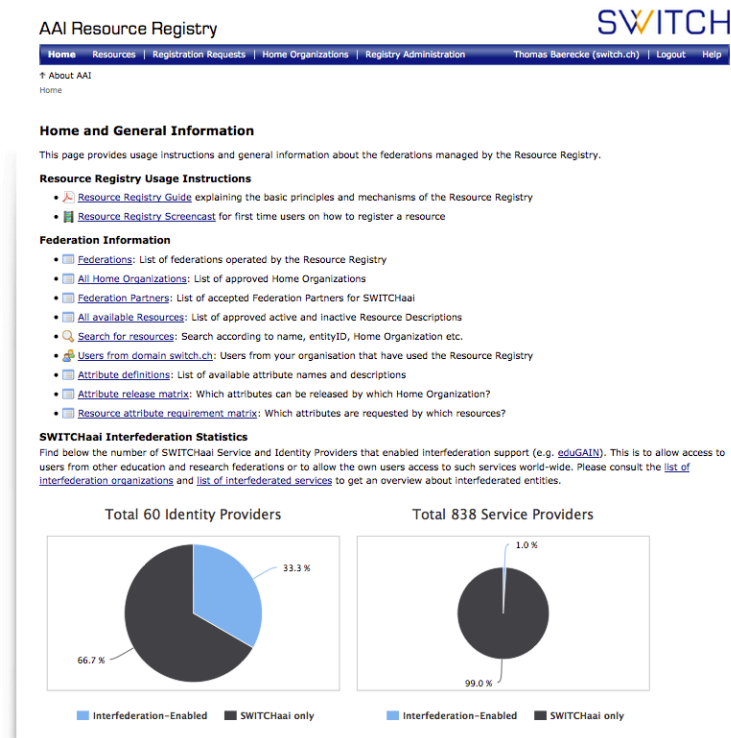
- Editing XML files by hand is error-prone and clumsy
- Managing the federation metadata by hand is cumbersome
- Legal processes should be technically supported
- Multiple federations must be managed

**A web-based tool to solve these problems!**

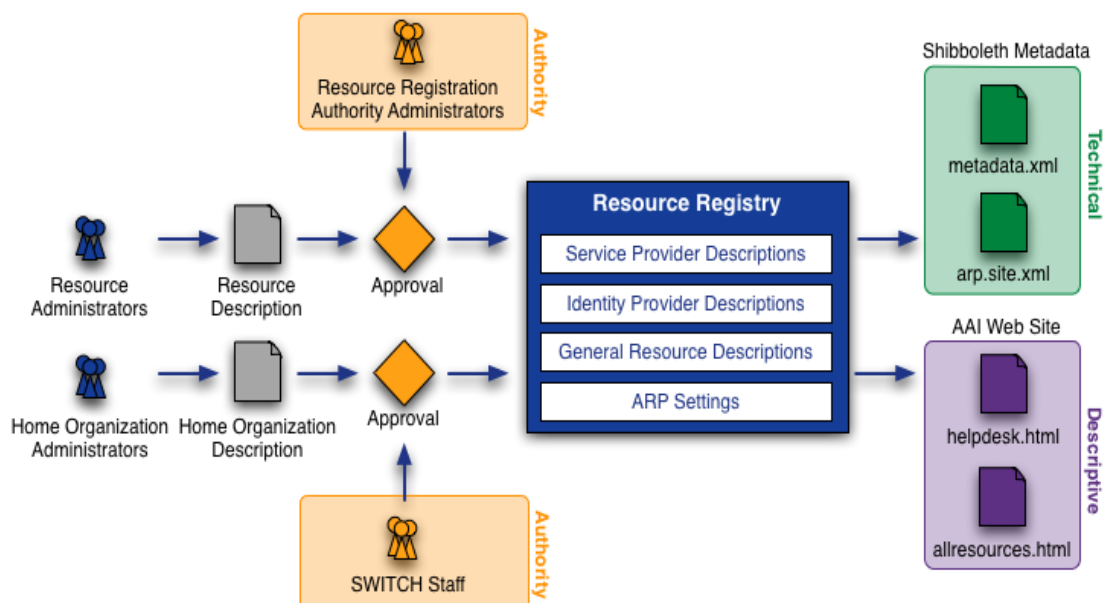
### Goals for such a Tool:

- Scalable metadata management
- Support administrative processes
- Provide auxiliary functions to support federation
- As little overhead as possible

## The AAI Resource Registry



# Resource Registry Processes



**Before an SP/IdP description becomes part of federation metadata, it must be approved by an authority first**

## Roles in the Resource Registry

- **Resource Registry Administrator**  
SWITCH staff members. Can edit/delete everything
- **Home Organisation Administrator**  
User that can manages the description/metadata of an organisation
  - **Attribute Administrator**  
Subset of privileges of Home Organisation administrator  
User that can change the attribute release policy of an organisation
- **Resource Administrator**  
Creates and manages descriptions of AAI services/Service Providers
- **Resource Registration Authority Administrator**  
Approves descriptions of AAI services/Service Providers

## Output of Resource Registry

- **Metadata**, see <http://www.switch.ch/aai/metadata/>
- **Configuration files** for IdPs and SPs (shibboleth2.xml, ...)
- **Helpdesk webpage** shows contact persons/helpdesk for your SP

### Your most recently used Resource's helpdesk

Contact the helpdesk of the Resource you wanted to connect to, if you experience **problems after successful login**.

#### Forge: Project Hosting Platform

Support Contact: [SWITCHaai Team](#), +41 44 268 15 05

Find the Resource in the [list of Resources grouped by Home Organization](#) or in the [long list of all public Resources](#).

- **Public Resource list**, see <http://www.switch.ch/aai/participants/>

#### AAI Wiki - Waaikiki

No Helpdesk web page specified

[Show contact persons](#)

[Show requested attributes](#)

[Show intended audience](#)

[en] AAI Wiki - Waaikiki

## AAI Attributes



# SWITCH

SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)

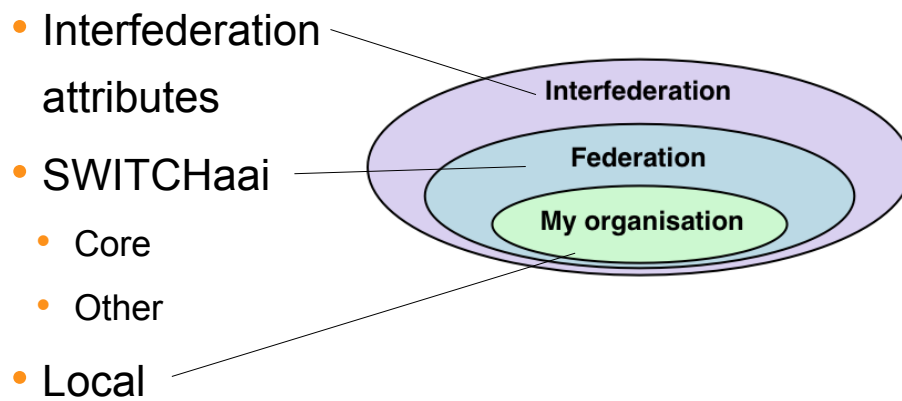
# Agenda

- attribute usage
- attribute scope
- user identifier attributes

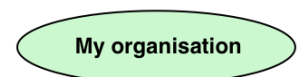
## Attribute usage

- identification
- authorisation
  - Access decision based on attribute values
  - individual or role based access control
- additional user information
  - Portal personalization e.g. preferred language

## Attribute scopes



## Attribute examples



Local scope:

**Group membership** at the Uni Lausanne

SAML2 Name:

urn:oid:2.16.756.1.2.5.1.1.1003

SAML1 Name: urn:mace:switch.ch:SWITCHaai:unil.ch:unilMemberOf

# Attribute examples

Federation

SWITCHaai scope:

**Study branch 1** (swissEduPersonStudyBranch1)

Study branch of a student, first level of classification

SAML2 Name:

urn:oid:2.16.756.1.2.5.1.1.6

SAML1 Name:

urn:mace:switch.ch:attribute-def:swissEduPersonStudyBranch1

## SWITCHaai Attributes

Federation

### Personal

Unique Identifier

Surname

Given name

E-mail

Persistent ID

User ID

Matriculation number

Employee number

Address(es)

Phone number(s)

Preferred language

Date of birth

Card UID

### Group Membership

Home Organization Name

Home Organization Type

Affiliation

Study branch

Study level

Staff category

Group membership

Organization Path

Organizational Unit Path

### Implementation of Attributes

- Core Attributes

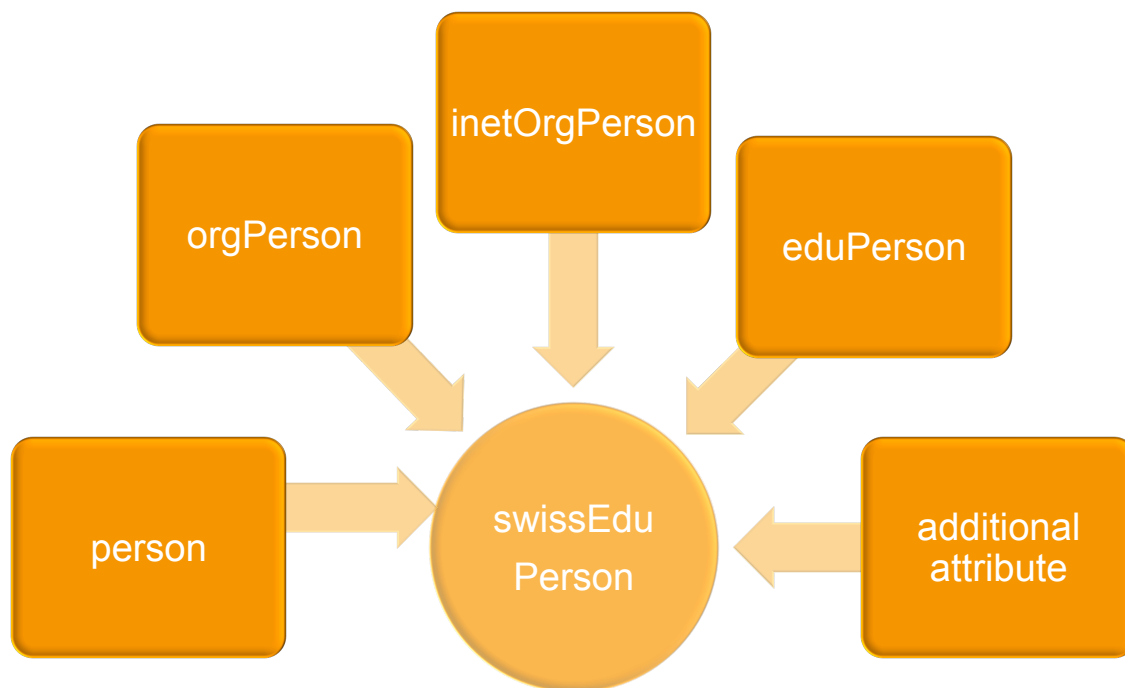
- Other Attributes

<https://switch.ch/aai/attributes>

[https://www.switch.ch/aai/docs/AAI\\_Attr\\_Specs.pdf](https://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf)

## swissEduPerson definition

Federation



## Attribute examples

Federation

SWITCHaai scope:

**Affiliation** (eduPersonAffiliation)

SAML2 Name:

urn:oid:1.3.6.1.4.1.5923.1.1.1.1

Since 2012:

The **member** affiliation MUST be asserted for people carrying one or more of the following affiliations: faculty or staff or student.



## Standardized Attributes

Interfederation

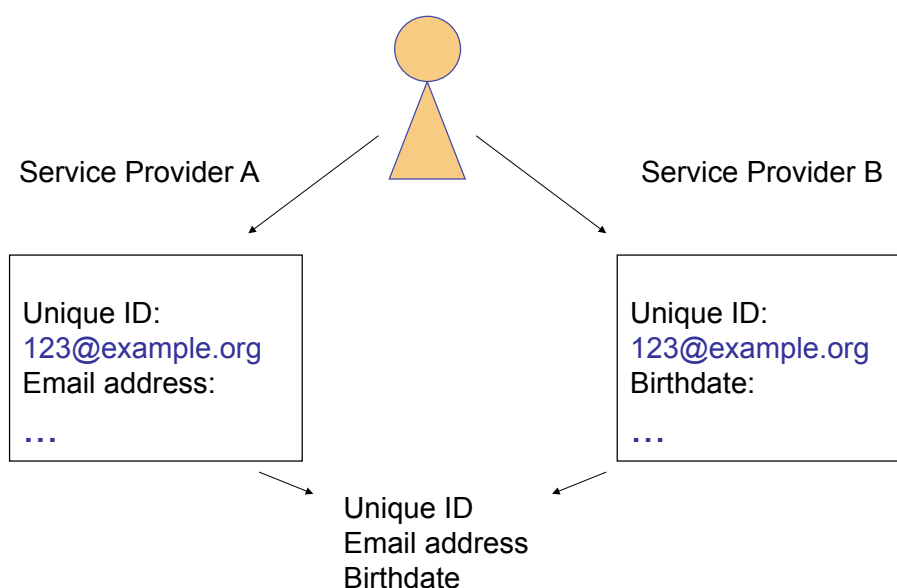
- Relevant for communication with entities from other federation via eduGAIN (or on bilateral basis)

| Friendly name                                      | Defined in | Example  |
|--|------------|--|
| displayName  | eduPerson  | Beatrice Huber   |
| common name (cn)                                   | eduPerson  | Beatrice Huber   |
| mail   | eduPerson  | bea.huber@switch.ch  |
| eduPersonAffiliation<br>eduPersonScopedAffiliation | eduPerson  | staff<br>staff@switch.ch   |
| eduPersonPrincipalName                             | eduPerson  | 234cd8z239@switch.ch   |
| schacHomeOrganization                              | SCHAC      | switch.ch  |
| schacHomeOrganizationType                          | SCHAC      | urn:mace:terena.org:schac:home<br>OrganizationType:int:NREN  |
| persistent Name ID/<br>eduPersonTargetedID         | eduPerson  | https://aai-logon.switch.ch/idp/shibboleth!<br>https://aai-viewer.switch.ch/interfederation-test/<br>shibboleth!<br>OV8woGYuxOafzuCSqvc15S5NdIU= |

## User identifier attributes

Federation

- Using account linking, the data is worth even more.



## persistent ID (eduPersonTargetedID)

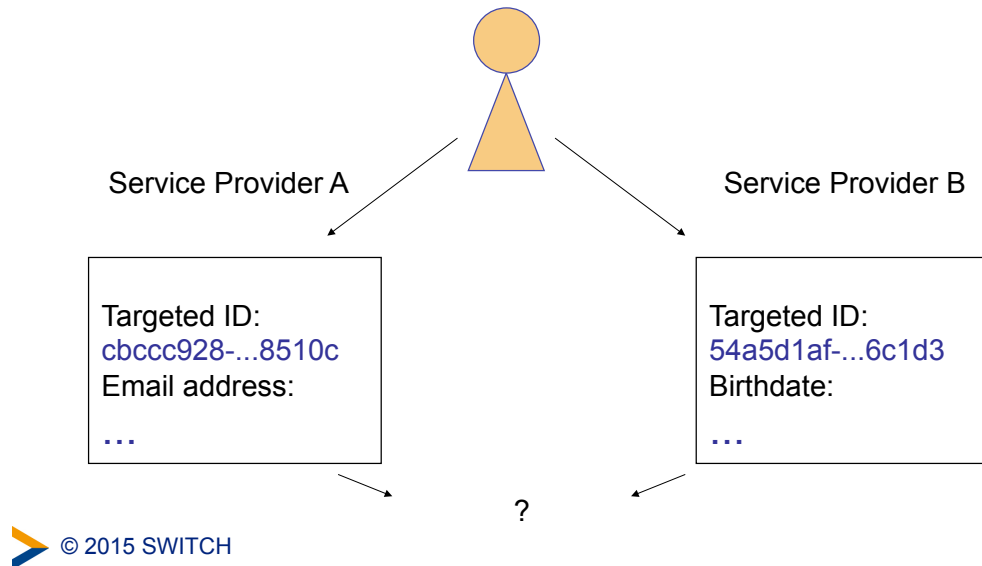
Federation

### Example persistent ID

`https://idp.example.org/idp/shibboleth!`

`https://sp.example.org/shibboleth!`

`f74698d6-854c-480c-b566-702006318cc3c`



## Email vs persistent ID vs Unique ID

Federation

| Properties   | Email | Unique ID | persistent ID |
|--------------|-------|-----------|---------------|
| scoped       | ✓     | ✓         | ✓             |
| persistent   | ✓     | ✓         | ✓             |
| opaque       | ✗     | ✓         | ✓             |
| non-reusable | ✗     | ✓         | ✓             |
| targeted     | ✗     | ✗         | ✓             |
| revocable    | ✗     | ✗         | ✓             |

# Interfederation



# SWITCH

SWITCHaai Team  
aai@switch.ch

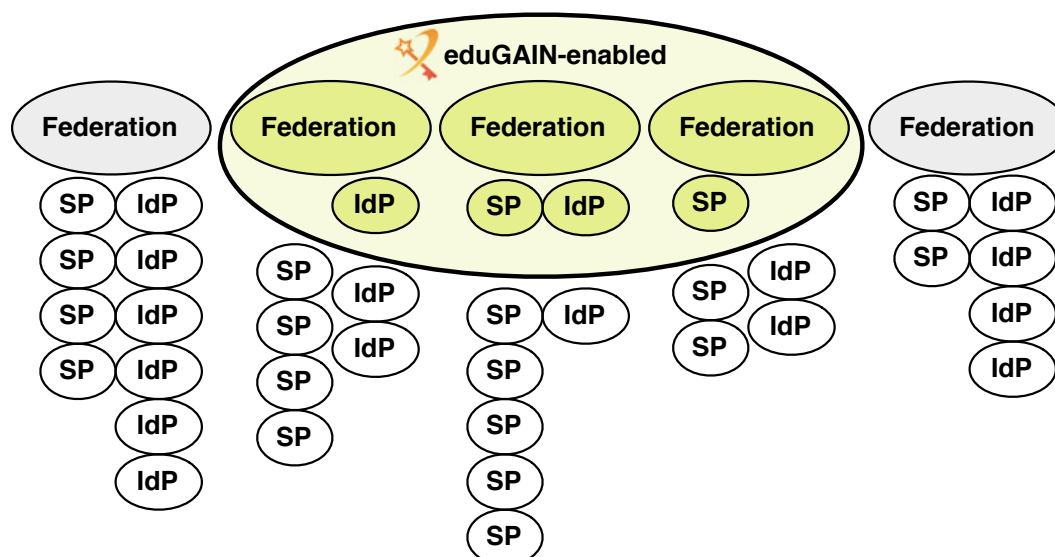
## Agenda

- Why Interfederation?
- Status
- Scalable Attribute Release
- GÉANT Data Protection Code of Conduct & Privacy Policy
- How to Interfederate in SWITCHaai?

# Why Interfederation?

- Federations are mostly of national scope
    - Services may need to register in multiple federations to serve all their users. That's time consuming and becomes a huge overhead.  
e.g. EBSCO Publishing is registered in 22 federations!
  - Research projects are mostly multi-national
  - **Interconnecting national federations → Interfederation**
- Register the IdP or SP in only one federation and enable it for interfederation
- Enable the IdP for interfederation
    - Its users will be able **access services from other federations**
  - Enable the SP for interfederation
    - The service can **serve users from other federations**

## eduGAIN Adoption Width vs. Depth



- Good federation adoption (Width)
- Entity Adoptions (Depth) is growing
- Not every SP has requirements to interfederate

## Interfederation Status

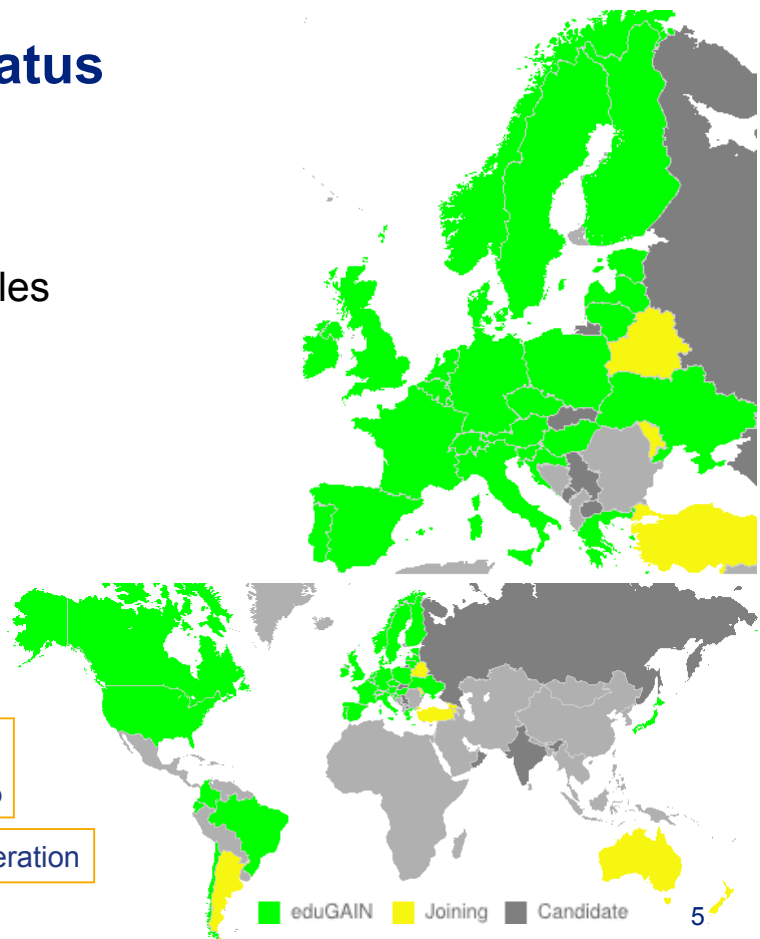
- eduGAIN is the GÉANT Interfederation Service
- eduGAIN design principles
  - Low barrier to entry
  - No requirements to change local standards/procedures
  - Minimal central infrastructure
- Status August 2015
  - Total: 1412 IdPs, 965 SPs
  - From SWITCHaai: 20 IdPs, 8 SPs

<http://www.edugain.org>

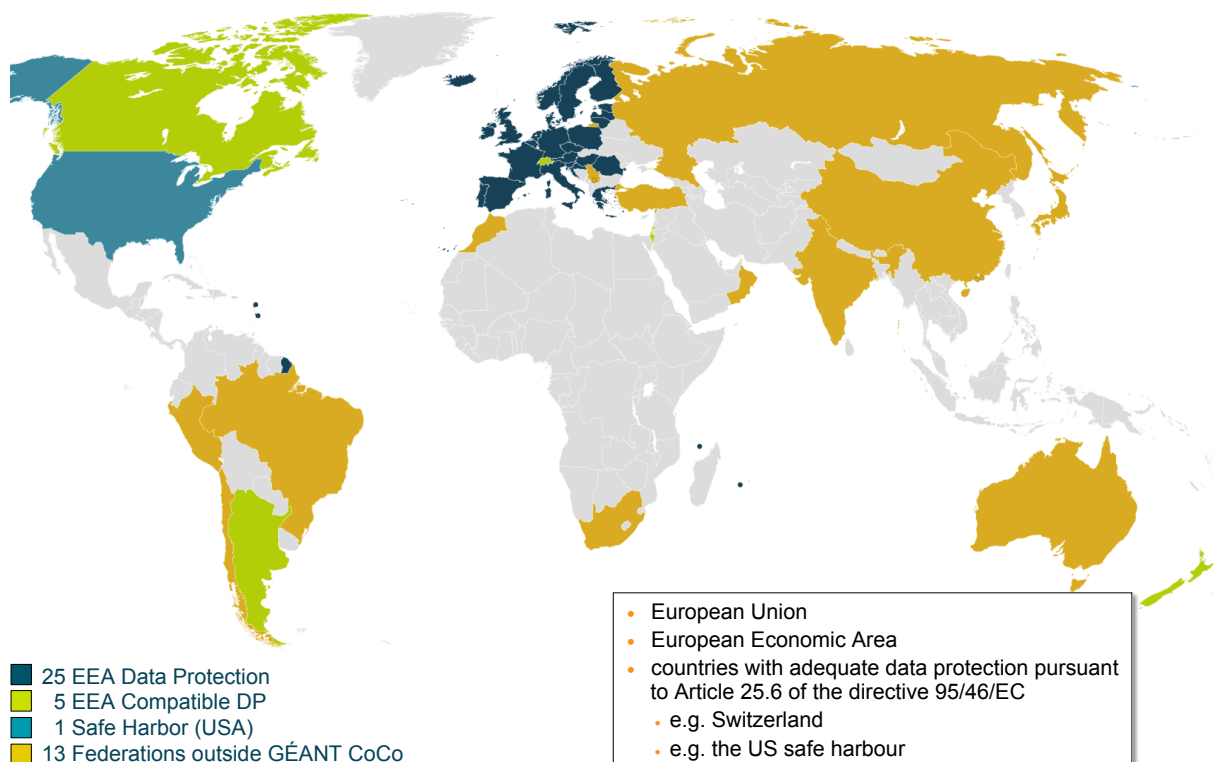
<https://technical.edugain.org/status.php>

<https://www.switch.ch/aai/interfederation>

© 2015 SWITCH



## Federations & GÉANT Data protection Code of Conduct



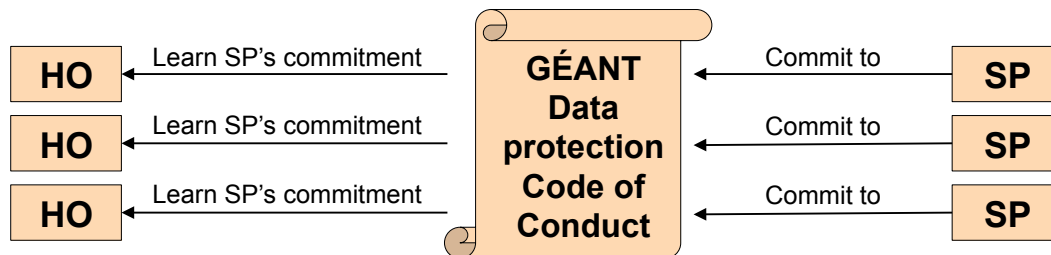
© 2015 SWITCH

6

## GÉANT Data Protection Code of Conduct

### Increase the trust in Service Providers (SPs)

- The method is based on the EU Data Protection directives
- The SP has to provide a Privacy Policy (in English, according to the guideline)
- That will encourage the Home Organisation IdP to release attributes
  - ➔ attribute release will scale



### Code of Conduct Toolkit

- **Data Protection Code of Conduct for SPs in EU/EEA**
- Entity category attribute definition for the Code of Conduct
- SAML2 profile for the Data Protection Code of Conduct

## Data Protection Code of Conduct (DP CoCo)

### Normative documents

- [Data Protection Code of Conduct for SPs in EU/EEA](#)
- Entity category specification for the DP CoCo
- SAML2 profile for the DP CoCo

<http://www.geant.net/uri/dataprotection-code-of-conduct/v1/>

### Non-normative, informational documents

- Introduction
- Introduction to the DP directive
- Managing DP risks using CoCo
- [Privacy policy guidelines for SPs](#)
- What attributes can an SP request
- [DP good practice for Home Organisations](#)
- Federation operator guidelines
- Handling non-compliance
- [IdP inform/consent GUI guidelines](#)

<https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home>

### Cookbook for DP CoCo

[https://wiki.edugain.org/Data\\_Protection\\_Code\\_of\\_Conduct\\_Cookbook](https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook)

# The Steps to Interfederate in SWITCHaai

- 1) Once per SWITCHaai Participant from the SWITCH Community a signature is required (see next slide)
- 2) SWITCH will set the 'flag' in the Resource Registry
- 3) Now, SP and IdP administrators can opt-in for interfederation;
  - First adapt the SP or IdP configuration according to the "Enabling Interfederation Support" guides
  - The IdP administrator configures user consent
  - Finally the administrator can click the checkbox in the Resource Registry!

| Interfederation |   |
|-----------------|---|
| Interfederation | <input checked="" type="checkbox"/> Enable interfederation for this resource<br>Activate this checkbox if the resource shall be accessed by users from non-SWITCHaai organizations. |

| Interfederation |   |
|-----------------|---|
| Interfederation | <input checked="" type="checkbox"/> Enable interfederation for this Home Organisation<br>Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources. |

<https://www.switch.ch/aai/interfederation>

## SWITCHaai Interfederation Access Declaration

Signing the Interfederation Access Declaration asserts:

- 1) the institution is aware of the additional data protection requirements when releasing personal data beyond SWITCHaai participants.
- 2) the institution acknowledges that it is liable for the actions of its End Users according to the "Service Regulations for Services by SWITCH" and the "SWITCHaai Service Description"
- 3) that the IdP supports user consent (for IdPv2 install uApprove)
- 4) the SPs will adhere to the "Data Protection Code of Conduct" (CoCo) and implement a Privacy Policy along the CoCo-criterias

<https://www.switch.ch/aai/interfederation>  
[https://wiki.edugain.org/How\\_to\\_write\\_the\\_privacy\\_policy](https://wiki.edugain.org/How_to_write_the_privacy_policy)

# VHO & Swiss edu-ID

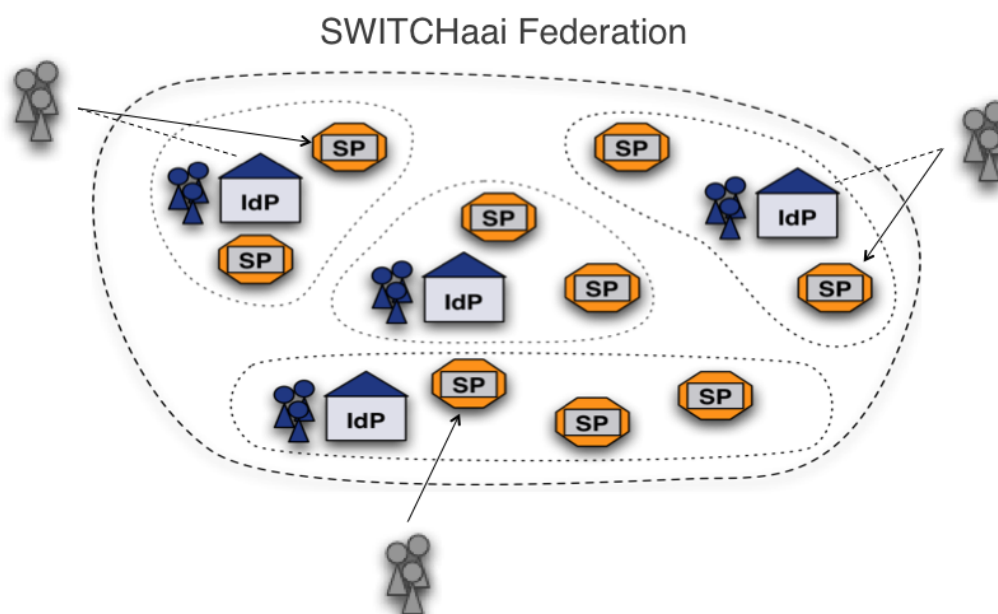


# SWITCH

SWITCHaai Team  
aai@switch.ch

## Motivation – loose relationships

2





## Possible solutions

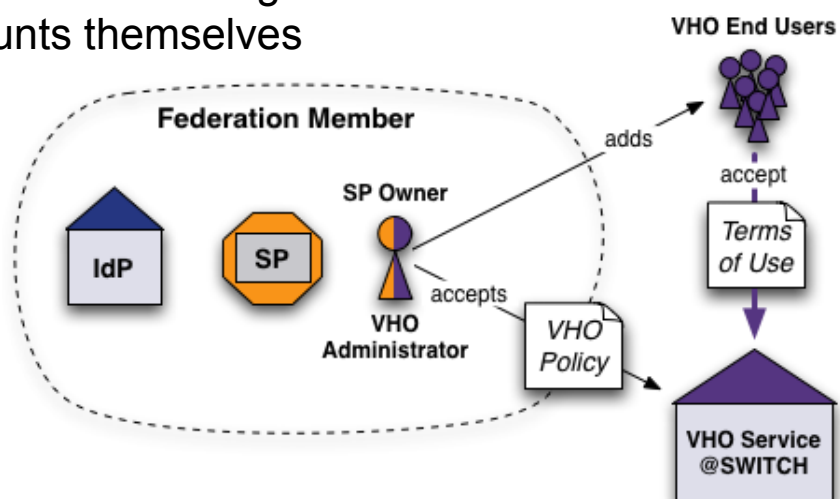
3

| VHO   | Swiss edu-ID   |
|---|--|
| +   | +  |
| <ul style="list-style-type: none"> <li>• “Regular” SWITCHaai accounts</li> <li>• Included in WAYF / discovery service</li> <li>• Managed service</li> </ul> | <ul style="list-style-type: none"> <li>• Users can register themselves</li> <li>• Included in WAYF / discovery service</li> <li>• Scales well with many users</li> <li>• One account for all services</li> <li>• Future-proof</li> </ul> |
| -   | -  |
| <ul style="list-style-type: none"> <li>• Administrative overhead</li> <li>• Scaling with many users</li> <li>• One account per service</li> </ul>           | <ul style="list-style-type: none"> <li>• Limited control over the attributes and data quality</li> </ul>   |

## SWITCH VHO Service

4

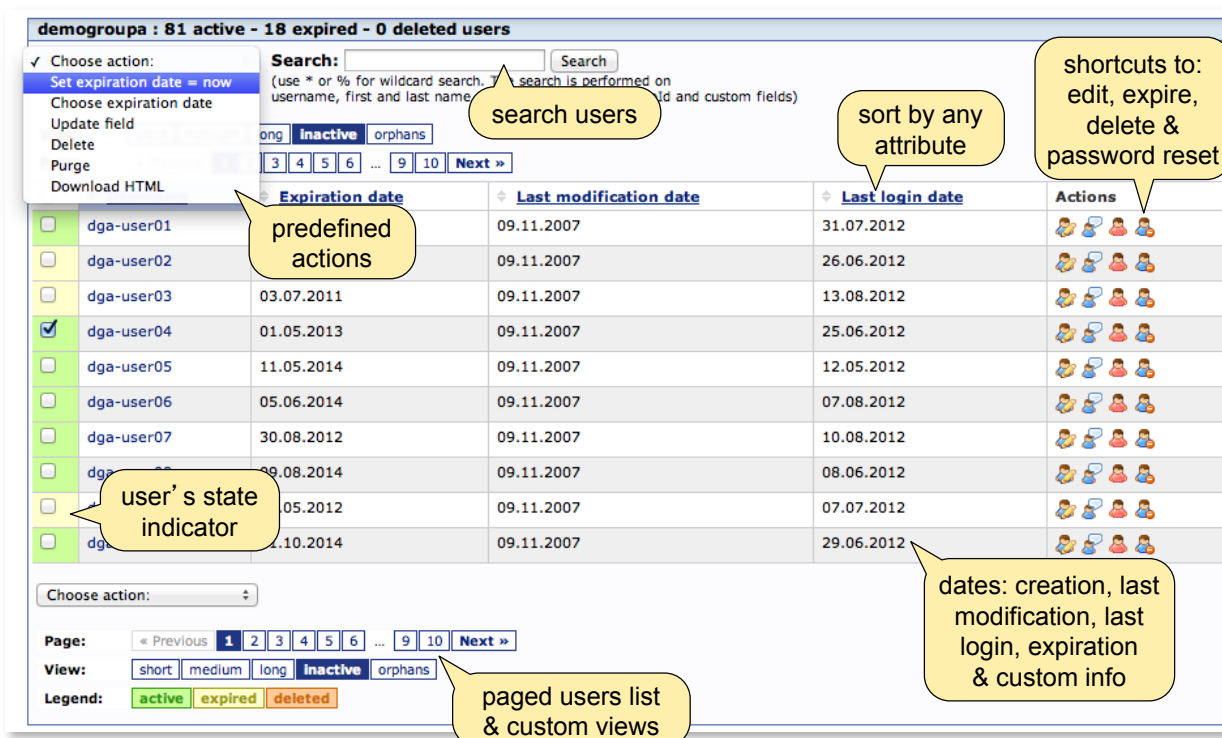
- Targeted end user groups
  - Attendees of a further education or other training
  - Collaboration projects from private companies or foreign universities, which are not in the SWITCHaai federation
- Groups are created by SWITCH
- Resource owners can manage end user accounts themselves



## VHOtools - Key functionalities

- Administrator services
  - Manage one or more groups, which can be structured hierarchically
  - Define description for each group (support contact, mail templates)
  - Create new user accounts with some AAI attributes (E-Mail, entitlement, ...)
  - Modify, delete and expire user accounts (incl. password resets)
  - Import and export of user lists
  - View group statistics
  - Account expiration reminder
- End user services
  - Login
  - User self-service password changes
  - Support information

## Screenshots VHO tool (1)

































**demogroupa : 81 active - 18 expired - 0 deleted users**

Choose action: ☒ Set expiration date = now  
☐ Choose expiration date  
☐ Update field  
☐ Delete  
☐ Purge  
☐ Download HTML

Search:  Search  
 (use \* or % for wildcard search. search is performed on username, first and last name, email address and custom fields)

long inactive orphans

3 4 5 6 ... 9 10 Next »

|  | Expiration date | Last modification date | Last login date | Actions   |
|--|-----------------|------------------------|-----------------|---|
| <input type="checkbox"/> dga-user01            |                 | 09.11.2007             | 31.07.2012      |    |
| <input type="checkbox"/> dga-user02            |                 | 09.11.2007             | 26.06.2012      |    |
| <input type="checkbox"/> dga-user03            | 03.07.2011      | 09.11.2007             | 13.08.2012      |    |
| <input checked="" type="checkbox"/> dga-user04 | 01.05.2013      | 09.11.2007             | 25.06.2012      |    |
| <input type="checkbox"/> dga-user05            | 11.05.2014      | 09.11.2007             | 12.05.2012      |    |
| <input type="checkbox"/> dga-user06            | 05.06.2014      | 09.11.2007             | 07.08.2012      |    |
| <input type="checkbox"/> dga-user07            | 30.08.2012      | 09.11.2007             | 10.08.2012      |    |
| <input type="checkbox"/> dga-user08            | 09.08.2014      | 09.11.2007             | 08.06.2012      |    |
| <input type="checkbox"/> dga-user09            | 05.2012         | 09.11.2007             | 07.07.2012      |    |
| <input type="checkbox"/> dga-user10            | 10.2014         | 09.11.2007             | 29.06.2012      |    |

Choose action:

Page: « Previous 1 2 3 4 5 6 ... 9 10 Next »

View: short medium long inactive orphans

Legend: active expired deleted

Annotations:

- search users
- sort by any attribute
- shortcuts to: edit, expire, delete & password reset
- predefined actions
- user's state indicator
- dates: creation, last modification, last login, expiration & custom info
- paged users list & custom views

## Screenshots VHO tool (2)

7

Create or modify  
user accounts  
using web forms...

demogroupa : Edit user

Fields marked with an asterisk (\*) are mandatory.

Username

dga-user06

uniqueID

d642431@test.vho-switchaa.ch

Last name \*

Walker

First name \*

William

E-mail \*

William.Walker@dga.edu.us

Entitlement \*

http://example.edu.org/dga

Business phone number

+1 4444 333 22 06

Business postal address

Golden Lane 6  
6000 San Francisco

Preferred Language

en

Description

Affiliation

affiliate

Home organization

vho-switchaa.ch

Home organization type

vho

Expiration date

or enter date 05.06.2014

Custom field 1

Custom field 2

Cancel

Save

demogroupa : View active user

Expire

Delete

Reset password

Edit

Username:

dga-user06

uniqueID:

d642431@test.vho-switchaa.ch

Last name:

Walker

First name:

William

E-mail:

William.Walker@dga.edu.us

Entitlement:

http://example.edu.org/dga

Business phone number:

+1 4444 333 22 06

Business postal address:

Golden Lane 6  
6000 San Francisco

Preferred Language:

en

Affiliation:

affiliate

Home organization:

test.vho-switchaa.ch

Home organization type:

vho

Expiration date:

05.06.2014 14:03:11

Creation date:

09.11.2007 15:48:35

Last modification date:

09.11.2007 15:48:35

Last login date:

07.08.2012 14:03:11

© 2015 SWITCH

## Screenshots edu-ID (1/2)

8

Registration

[Login](#) | [About](#) | [Help](#) | [Terms of Use](#)

Account Creation

2 E-mail Verification

3 Account Activation

Please complete the following form to create a new Swiss edu-ID account.

Authentication Data

E-mail Address

thomas.baerecke@switch.ch

Password

\*\*\*\*\*

Password is strong

Confirm Password

\*\*\*\*\*

How much is:

16

Personal Data

First Name

Thomas

Last Name

Baerecke

I fully understand and accept the [Terms of Use](#) for creating and using a Swiss edu-ID account.

The Terms of Use will also be sent to you by e-mail when your account has been successfully created.

Create Swiss edu-ID account

© 2015 SWITCH and [licensed content](#) / [Legal notice](#) / [Imprint](#)

Registration

[View and Modify Account](#) | [About](#) | [Help](#) | [Terms of Use](#)

Account Creation

2 E-mail Verification

3 Account Activation

✓ Your Swiss edu-ID account was successfully registered. Before it can be activated, the E-mail address you provided has to be verified. Therefore, an E-mail has been sent to the E-mail address [thomas.baerecke@switch.ch](mailto:thomas.baerecke@switch.ch). Please follow the instructions in the E-mail in order to confirm your E-mail address.

Due to SPAM filters it may take a few minutes until you receive the e-mail. If you do not receive the e-mail within 10 minutes, please also check your SPAM folder.

© 2015 SWITCH and [licensed content](#) / [Legal notice](#) / [Imprint](#)

Registration

[Login](#) | [About](#) | [Help](#) | [Terms of Use](#)

Account Creation

2 E-mail Verification

3 Account Activation

✓ Your E-mail address [thomas.baerecke@switch.ch](mailto:thomas.baerecke@switch.ch) was successfully verified and your Swiss edu-ID account is now active. You should soon receive an E-mail message with further details.

When asked to authenticate at the login page of the Swiss edu-ID; use as login name the E-mail address and the password that you provided during account creation. By changing your Swiss edu-ID account you can add further E-mail addresses that are then associated to your Swiss edu-ID.

View Account Details

© 2015 SWITCH and [licensed content](#) / [Legal notice](#) / [Imprint](#)

© 2015 SWITCH

## Screenshots Swiss edu-ID (2/2)

Access your Swiss edu-ID Account

SWITCH

[View and Modify Account](#) | [About](#) | [Help](#) | [Terms of Use](#)

Authentication

Account Data

Your Swiss edu-ID account was successfully changed and saved.

This page allows you to update and extend your Swiss edu-ID account.

### Account Completeness

Your Swiss edu-ID account is 54% complete: |||||

Check what information at maximum is released about you by [accessing the AAI Attribute Views](#).

| Personal Data      |          | Quality | Actions |
|--------------------|----------|---------|---------|
| First Name         | Thomas   |         |         |
| Last Name          | Baerecke |         |         |
| Date of birth      |          |         |         |
| Gender             |          |         |         |
| Preferred Language | German   |         |         |

### Authentication Data

|          |       |  |
|----------|-------|--|
| Password | ***** |  |
|----------|-------|--|

### Contact Data

|                     | Quality  | Actions |
|---------------------|--|---------|
| E-mail              |  |         |
| Primary E-mail      | thomas.baerecke@switch.ch                                |         |
| Additional E-mail   |  |         |
| Business            |  |         |
| Business Address    | SWITCH<br>Wendstrasse 2<br>CH-8004 Zürich<br>Switzerland |         |
| Business Phone      | +4142681634  |         |
| Private             |  |         |
| Home Address        |  |         |
| Home Phone          |  |         |
| Mobile Phone Number |  |         |

### Linked Identities

|  | Quality          | Actions |
|--|------------------|---------|
| Institutional Identities   |                  |         |
| SWITCHaaI Identity   | switch.ch        |         |
| SWITCHaaI Affiliation  | member@switch.ch |         |
|  | staff@switch.ch  |         |
| <div>  SWITCHaaI Affiliations can be added by adding additional SWITCHaaI identities. </div> |                  |         |
| Other Identities   |                  |         |
| ORCID Identifier   |                  |         |

© 2015 SWITCH and [licensed content](#) / [Legal notice](#) / [Imprint](#)



# SP Hands-on Session

# Installing and Configuring a Shibboleth 2 Service Provider



The logo for SWITCH, featuring the word "SWITCH" in a bold, blue, sans-serif font. The letter "W" is stylized with a yellow and orange gradient.

## Serving Swiss Universities



## Credits and General Information

2

- Slides were originally created by Scott Cantor, Internet 2 Developer of the Shibboleth Service Provider
- Course material is adapted for use in SWITCHaai
- Course material is published online
- If you see this  on a slide, hands-on work is required
- URLs at bottom right point to pages with more details
- On slides with  separate presentations focus on special topic

## Main Goals of Hands-On Session

3

- Install and configure a Shibboleth Service Provider 2
- Register it with the AAI Test federation
- Know how and where to configure things
- Learn how to protect static web pages
- Understand how attributes can be used in web applications

## Essential OS Commands for Linux

4

| DOS Command                    | Linux Command                             |
|--------------------------------|---|
| dir                            | ls -l                                     |
| cd <directory>                 | cd <directory>                            |
| mkdir <b>or</b> md <directory> | mkdir <directory>                         |
| rmdir <b>or</b> rd <directory> | rmdir <directory>                         |
| chdir                          | pwd                                       |
| del <b>or</b> erase <file>     | rm <file>                                 |
| copy <b>and</b> xcopy <file>   | cp <b>and</b> cp -R <file>                |
| find <b>or</b> findstr <file>  | grep <string> <file>                      |
| comp <file1> <file2>           | diff <file1> <file2>                      |
| edit <file>                    | nano <b>or</b> vim <b>or</b> emacs <file> |
| ping <host>                    | ping <host>                               |
| reboot                         | reboot                                    |

 © 2015 SWITCH

## Tips and Tricks for Hands-On Session

5

- The password usually is "password"
- Lines starting with \$ are commands to be executed
  - Replace # with a number (your participation number during the training)
- Command should be executed as root user
  - Happens automatically if Terminal is opened or if text editor is used
- Character \ is line break symbol, which allows to break a line when typed
- Watch out for invalid XML/configuration errors
  - Consult Debugging SP Handout for hints to resolve problems

 © 2015 SWITCH

## More Tips and Tricks for Hands-On Session

6

- Restart the Shibboleth daemon shibd after every change
  - shibd automatically reloads config but only restarts "reveal" errors
  - Alternatively, look at the log file for errors
- Delete session cookies after changes (or restart browser)
  - Should not be necessary but is safer for testing
- SSH access to connect to your VM (only with VirtualBox)

```
$ ssh -p 2222 sp-admin@127.0.0.1
```

The password is 'password', user is in sudoers list  
Useful for `$ tail -f /var/log/shibboleth/shibd.log`
- On the VM you will find a web page with useful bookmarks  
In your web browser open: `https://sp#.example.org/`

## Test Users on AAI Demo Home Organisation

7

- Username: g.utente      Password: password

```
Givenname surname: Giovanni Utente
Affiliation:         faculty;member
Entitlements:        http://example.org/res/99999
                    http://publisher-xy.com/e-journals
```
- Username: p.etudiant      Password: password

```
Givenname surname: Pière Edudiant
Affiliation:         student;member
Entitlements:        urn:mace:dir:entitlement:common-lib-terms
                    http://www.example.org/aai/agreement-2011
```
- Username: h.mitarbeiter      Password: password

```
Givenname surname: Hans Mitarbeiter
Affiliation:         staff;student;member
Entitlements:        urn:mace:dir:entitlement:common-lib-terms
                    http://www.example.org/vip
```

# VM Operating System Environment

8

- Ubuntu 14.04 LTS, Virtual Box/VMWare VDK image
- User: "**sp-admin**" / Password: "**password**" (in sudoers list)
- Apache 2 on ports 80 (http) and 443 (https)
- Self-signed SSL web server certificate
- AuthConfig added to /cgi-bin and /html for .htaccess
- Hostnames:
  - `sp#.example.org`
  - `altsp#.example.org` (alternative hostname)

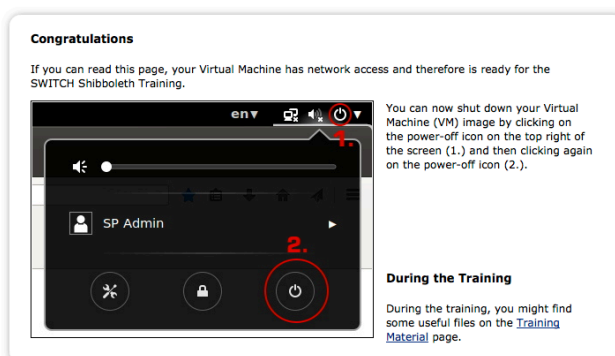


## Boot up the image



9

1. Open "SWITCH-Shibboleth-Training.vbox" image in Virtual Box
2. Start the virtual machine (VM)
3. After login, Firefox will open automatically.  
Ensure that it displays this page:



If you don't see this message, contact an assistant.





## VM Setup

 10

### 4. Open a Terminal



### 5. Enter "password" to become root user.

### 6. Then execute:

```
$ setupVM
```

### 7. Enter your participation number from the name tag

VM will then reboot automatically after a few seconds.

 © 2015 SWITCH

## Do the AAI Demo as a Quick Test

 11

AAI Demo

SWITCH

↑ About AAI

**Area: Any authenticated user**  
Shibboleth Service Provider, current <RequestMap />:

```
<Path
  name="secure"
  authType="shibboleth"
  requireSession="true">
</Path>
```

| Attributes  | Values   |
|---|--|
| <b>persistent-id</b><br>SAML2 Attribute Name:<br>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent | https://aai-demo-idp.switch.ch/idp/shibbolethhttps://aai-demo.switch.ch/shibbolethw7fSr2mQ19h1XhYqFEnq9LazHUM= |
| <b>uniqueID</b><br>SAML2 Attribute Name:<br>urn:oid:2.16.756.1.2.5.1.1.1                              | 234567@aai-demo-idp.switch.ch  |
| <b>givenName</b><br>SAML2 Attribute Name:<br>urn:oid:2.5.4.42   | Demouser   |

1. In Firefox, open [aai-demo.switch.ch](https://aai-demo.switch.ch)
2. Click on "Any authenticated user"
3. Select the "AAI Demo Home Organisation"
4. Log in using a test user (e.g. "g.utente" "password")

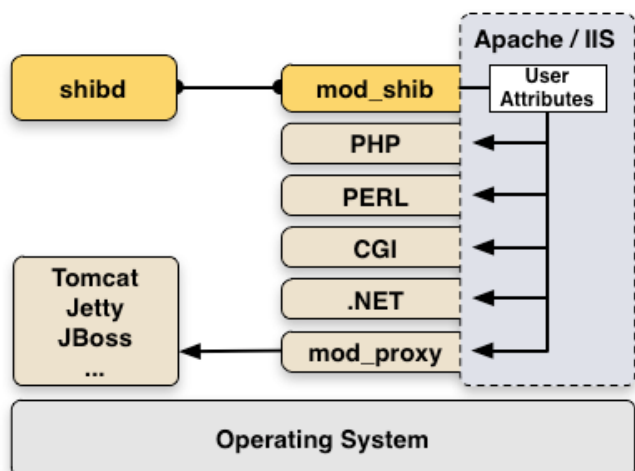
 © 2015 SWITCH

## Goals:

1. Terminology and SP Overview
2. Installation
3. Configuration
4. Quick Sanity Check

## Shibboleth SP: Daemon & mod\_shib

- Runs on: Linux, Solaris, Windows, Mac OS X, FreeBSD, ...
- Protects web applications
- shibd processes attributes
- Can authorize users with
  - Apache directives
  - Shibboleth XML Access rule
- Provides attributes to applications



## Terminology

- **Service Provider (SP)**  
Consumes SAML assertions, protects web applications
- **Identity Provider (IdP)**  
Asserts digital identities using SAML
- **Discovery Service/WAYF (DS/WAYF)**  
Lets user choose Identity Provider/home organisation
- **shibd** (Shibboleth daemon)  
SP service/daemon for maintaining state
- **Session**  
Security context and cached data for a logged-in user
- **Session Initiator**  
Part of SP that controls how SSO requests are started

## SWITCHaai Deployment Guides

### How to install Shibboleth?

- Instructions SWITCHaai and AAI Test federations:  
<https://www.switch.ch/aai/guides/sp/>
  - Separation between installation and configuration.
  - Instructions for all major operating systems
  - SWITCHaai guides are custom-tailored and easier!
- General instructions on Shibboleth Wiki:  
<https://wiki.shibboleth.net/confluence/display/SHIB2/Installation>
  - Comprehensive documentation on most features
  - Not targeted for a specific federation

# Deployment Guides

 16

- In Firefox (on the VM) open: <http://www.switch.ch/aai/>
- Find the page with the Service Provider Deployment
  - Or find the link on the bookmarks page



- Deployment Guide is split into:
  - **Installation Guide:** Custom tailored for all major operating systems
  - **Configuration Guide:** Independent from OS (except Windows)

 © 2015 SWITCH

# Service Provider Installation

 17

- Start with the "Installation Guide"

## Deployment Guides

Installation and Configuration Guides for the current Shibboleth Service Provider:

- [Shibboleth Service Provider Installation Guide](#) for Linux, Mac OS X and Windows.
- [Shibboleth Service Provider Configuration Guide](#) for the SWITCHaai and AAI Test federations.

- In section 1. "Introduction" select "Ubuntu" as operating system
  - Guide will adapt itself automatically depending on selected OS
- Proceed with sections 3 – 5 in the guide
  - Section 2 can be skipped (`sudo` and `curl` are already installed)
  - You must open a terminal window for these steps
  - Provide `sp#.example.org` for the `mod_shib` Test in section 5

 © 2015 SWITCH

## Installation

 18

- Open a Terminal window
  - Click on this icon in the launch bar at the left
- Proceed with sections 3 – 5
  - Provide `sp#.example.org` for the `mod_shib` Test in section 5
  - When running `sudo shibd -t` there will be some (expected) errors  
Just ensure that the Overall configuration is loadable
- **Service Provider is now installed but not configured yet!**



 © 2015 SWITCH

## Installation for Other Operating Systems

19

- On Debian/Ubuntu (by Debian/Ubuntu):  
`$ apt-get install libapache2-mod-shib2`
- On Mac OS X with MacPort (by Shibboleth team):  
`$ port install shibboleth`
- On Redhat/Suse/OpenSuse/CentOS (by Shibboleth team):  
`$ yum install shibboleth`
- On Windows with MSI packet (by Shibboleth team)
- Manual compilation not very difficult either
  - But more difficult to maintain efficiently

 © 2015 SWITCH

<https://wiki.shibboleth.net/confluence/display/SHIB2/Installation>

## Service Provider Binaries and Paths

20

- **Shibboleth Daemon binary**

Linux/Unix: `/usr/sbin/shibd`

Win: `C:\opt\shibboleth-sp\sbin\shibd.exe`

- **Shibboleth main configuration file**

Linux/Unix: `/etc/shibboleth/shibboleth2.xml`

Win: `C:\opt\shibboleth-sp\etc\shibboleth\shibboleth2.xml`

- **Shibboleth Libraries/Modules/Extensions**

Linux/Unix: `/usr/lib/shibboleth/*.so`

Win: `C:\opt\shibboleth-sp\lib\*.so`



## Important directories

21

- `/etc/shibboleth/`
  - Master and supporting configuration files
  - Locally maintained metadata files
  - HTML templates (to customize the look & feel of service)
  - Logging configuration files (\*.logger)
  - Credentials (certificates and private keys)
- `/var/run/shibboleth/` and `/var/cache/shibboleth/`
  - UNIX socket
  - remote metadata backups
- `/var/log/shibboleth/`
  - `shibd.log` and `transaction.log` files
- `/var/log/apache2/` or `/var/log/shibboleth/apache2/`
  - `native.log` (is written by `mod_shib` web server module)



# Configuration

 22

- Continue with Configuration Guide
  - "Configuration Guide for new installations" at bottom of installation guide

**Basic Configuration**  
Select the operating system:  
In which federation would you like to deploy your SP?  
Hostname ([Fully qualified domain name](#)) of the service?

☒ **Unix-based System** (including Mac OS X)  
☐ **Windows System**  
AAI Test (Development and Test) ▾  
sp#.example.org

- In Setup Profile
  - Select "AAI Test Federation"
  - Provide sp#.example.org as host name
  - Don't change the other values which were updated automatically
  - Click on "Update configuration guide with above Data"

 © 2015 SWITCH

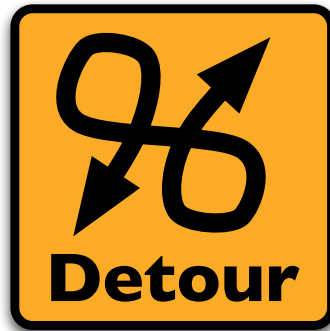
## EntityID of an SP

23

- Every SP needs a unique identifier: The **entityID**
- Where is entityID used?
  - In transmitted messages, local configuration, metadata
  - IdP log files, configuration, filtering policies
- EntityID should be: Unique, locally scoped, representative and unchanging
- Convention: Include FQDN of your service
  - Guide automatically sets the following entityID:  
https://sp#.example.org/shibboleth

 © 2015 SWITCH

Purpose and usage of certificates in SAML



Please consult the table of contents to find this presentation in your hand-outs.

## Generate X.509 Key/Certificate

- Script to generate certificate and private key:  
`/usr/sbin/shib-keygen` or `/etc/shibboleth/keygen.sh`
  - Runs automatically during installation on some OS
- Proceed with section 4 in the guide about the X.509 certificates
  - Generates an X.509 certificate according to SWITCHaai requirements
  - Results in `sp-cert.pem` and `sp-key.pem` in `/etc/shibboleth`
  - Have a look at the PEM encoded certificate with  
`$ less /etc/shibboleth/sp-cert.pem`
  - To see content of certificate, execute:  
`$ openssl x509 -text -in /etc/shibboleth/sp-cert.pem`



## Install and Test Configuration Files

 26

- **Continue with section 5, the 'Shibboleth Configuration'**
- This downloads:
  - Shibboleth main configuration (shibboleth2.xml)
  - Attribute map configuration (attribute-map.xml)
  - Attribute policy configuration (attribute-policy.xml)
  - SWITCHaai Root CA certificate to verify metadata signature
- Configuration files are custom-tailored for your Service Provider based on values in 'Setup Profile'
- **Run 'Configuration Tests' in section 6 of the guide**
  - Most important: Check Shibboleth configuration with: `$ shibd -t`



© 2015 SWITCH

<https://www.switch.ch/aai/support/certificates/embeddedcerts-requirements/>

## Sanity Checks

27

- Start processes:

```
$ /etc/init.d/shibd restart or $ service shibd restart
$ /etc/init.d/apache2 restart or $ service apache2 restart
```
- Check shibd status (XML should be returned on success):

```
$ curl -k --interface lo \
  https://sp#.example.org/Shibboleth.sso/Status
```
- Access session handler from your browser:

```
https://sp#.example.org/Shibboleth.sso/Session
```

After certificate warning, you get "A valid Session was not found" error
- See how a Shibboleth error looks like (you get an exception):

```
https://sp#.example.org/Shibboleth.sso/Foobar
```



© 2015 SWITCH

### Goals:

1. First attempt to login on Service Provider
2. Learn about Metadata
3. Learn about the AAI Resource Registry
4. Register Service Provider for AAI Test federation

## Configuration Files

- **Service Provider is now installed and configured**

- Let's see if authentication with AAI already works

- **Open in Firefox:**

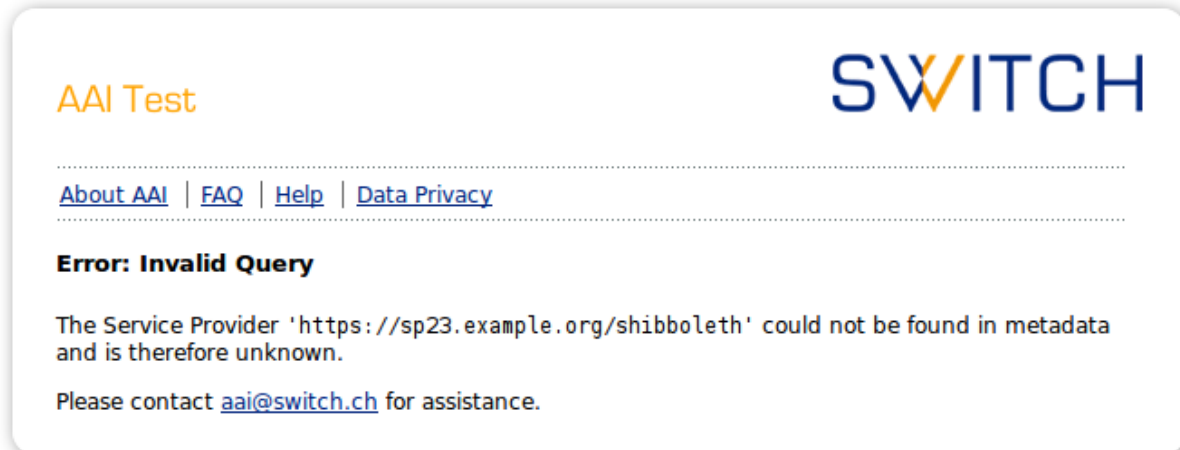
`https://sp#.example.org/Shibboleth.sso/Login`

- `/Shibboleth.sso/Login` is the default login initiator.  
It can be used to start the AAI login process
- Shibboleth will redirect you to the Discovery Service/WAYF
- You will see an error message

## Service Provider Not Yet in Metadata

30

Discovery Service (WAYF) and Identity Provider don't "know" your Service Provider yet because they don't have metadata about it.



## (Federation) Metadata


31

- SAML Metadata is an XML document
- Typically is provided by a federation operator (e.g. SWITCH)
- Contains descriptions of all SPs and IdPs:
  - **entityID**: The unique identifier of the entity
  - **Supported protocols**: E.g. SAML1, SAML2
  - **X.509 certificates**: Contain the public key of a key pair
  - **Endpoint URLs**: What URLs to query or send messages to
  - **Descriptive** information: E.g. Display name, description, logos
  - **Contact information**: e.g. for support
  - **Registration information**: Who registered this entity when

## (Federation) Metadata

 32

1. Have a look at it by opening (`view` or `gedit`) the file:  
`/var/cache/shibboleth/metadata.aaitest.xml`  
Look for entityID:  
`https://aai-demo-idp.switch.ch/idp/shibboleth`
2. Now also have a look at your SP's metadata by opening:  
`https://sp#.example.org/Shibboleth.sso/Metadata`  
SP can generate (technical) SAML metadata about itself
3. To get your Service Provider into the AAI Test metadata, it has to be registered with the AAI Resource Registry

 © 2015 SWITCH

## Resource Registry

33

Purpose of the SWITCHaai Resource Registry and how to use it



Please consult the table of contents to find this presentation in your hand-outs.

 © 2015 SWITCH

## Registration

 34

1. Continue with section 7 "Register Service Provider"
  - Use your regular AAI account to log in to the Resource Registry
  - If you don't have an AAI account:
    1. Click on "Login for AAI Test Federation" button
    2. Select the "AAI Demo Home Organisation"
    3. To authenticate use Username: `sp-training-admin`  
Password: `password`
2. Click on the "Resources" tab
3. Then on "Add a Resource Description"

**The description of your training SP will be deleted some time after the training.**

 © 2015 SWITCH

## Resource Description I

 35

The Shibboleth wizard can download an SP's metadata

- But not if the SP is behind NAT or firewall
  - Therefore, you have to provide metadata manually
1. Open in Firefox:  
`https://sp#.example.org/Shibboleth.sso/Metadata`
    - This should open the XML file in the gedit text editor
  2. Copy all XML and paste it into the text area on the Resource Registry above the button "Run Shibboleth 2.x wizard"
  3. Then hit the button "Run Shibboleth 2.x wizard"
    - "Descriptive Information", "Service Locations" and "Certificates" should now be green (=completed)

 © 2015 SWITCH

## Resource Description II

 36

4. Click on "Basic Resource Information":
  - Choose "aai-demo-idp.switch.ch" as Home Organisation.
  - Add a name and description for your Service Provider  
E.g. "Demo SP #", "SP used for improving my Shib knowledge"
  - Finally, click on "Save and Continue"
5. Click on "Contacts"
  - Complete the fields with your email address and contact info.
  - Finally, click on "Save and Continue"
6. Click on "Required Attributes"
  - Add as requires attributes: Targeted ID/Persistent ID, Surname, Given Name, E-Mail, Affiliation, Entitlement and PrincipalName
  - Finally, click on "Save and Continue"

## Resource Description III

 37

7. Click on "Intended Audience":
  - Click on "Set all to included".
  - Finally, click on "Save and Continue"
  - You now have completed the Resource Registry
8. Add a comment that you register this Resource Description in the context of the SP training.
9. Click on "Submit for Approval"
  - You should then see the Resource Registration Authority (RRA) administrators who have to approve your Resource Description
  - The RRA admins might ask you for the certificate fingerprint to prove that you generated the certificate
  - To get the certificate's SHA1 fingerprint, run:  

```
$ openssl x509 -fingerprint -in /etc/shibboleth/sp-cert.pem
```

## Test Access to Service Provider

 38

- Once the Resource Description is approved, you become admin
- SP's metadata is included in federation's metadata:
  - In real life, it can up to two hours after the approval of the Resource Description until metadata has propagated to all Identity Providers
  - During the training event, metadata propagation is max. 5 minutes

### Test Access

1. In Firefox, open the URL:  
`https://sp#.example.org/Shibboleth.sso/Login`
2. Select the "AAI Demo Home Organisation" on the WAYF
  - If you instead get an error, wait a few minutes more
3. Use "g.utente" and "password" as login name and password

 © 2015 SWITCH

## Service Provider Deployment Complete

39

- When you are back on the Shibboleth Session handler (`/Shibboleth.sso/Session`) and see the following ...

#### Miscellaneous

**Session Expiration (barring inactivity):** 480 minute(s)

**Client Address:** 127.0.0.1

**Sso Protocol:** urn:oasis:names:tc:SAML:2.0:protocol

**Identity Provider:** `https://aai-demo-idp.switch.ch/idp/shibboleth`

**Authentication Time:** 2014-02-03T16:41:01.963Z

**Authentication Context Class:** urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

**Authentication Context Decl:** (none)

#### Attributes

**affiliation:** 2 value(s)

**entitlement:** 2 value(s)

**givenName:** 1 value(s)

**mail:** 1 value(s) )

**persistent-id:** 1 value(s) ue(s)

**surname:** 1 value(s)

... then you successfully deployed your Service Provider 😊

 © 2015 SWITCH

## If all fails: Use Catch-Up Configuration

40

- Download the SP Catch-Up configuration from the training page:  
`https://www.switch.ch/aai/docs/training/`
- Extract Shibboleth SP configuration files with:  
`$ tar xvzf shib-sp-catchup.tgz -C / --overwrite`
- From now on use **#=1** as participation number,  
`sp1.example.org`

## Basic Configuration

41

### Goals:

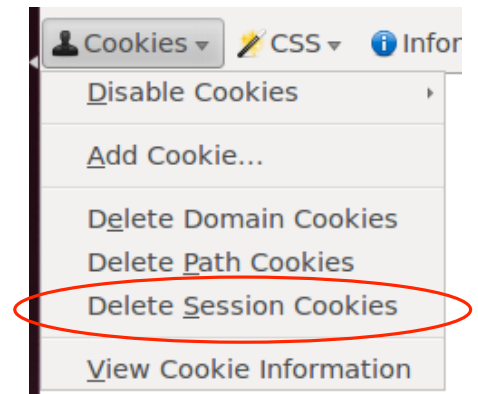
1. Local Logout
2. Understand purpose and structure of SP configuration files
3. Increase log level to DEBUG
4. Make a few simple configuration changes



## Logging Out

 42

- To logout locally from the SP and kill your session:  
`https://sp#.example.org/Shibboleth.sso/Logout`  
But this won't delete your session on the IdP!
- **Close the browser and restart it again!**  
Still the easiest and safest method for most web browsers
- Or delete all your session cookies  
For testing and development purposes use the "Firefox Web Developer" extension (installed on VM).



 © 2015 SWITCH

## Configuration Files in /etc/shibboleth

43

- **shibboleth2.xml** – main configuration file
- **attribute-map.xml** – attribute handling
- **attribute-policy.xml** – attribute filtering settings
- **\*.logger** – logging configuration
- **\*Error.html** –HTML templates for error messages
- **localLogout.html** – SP-only logout template
- **globalLogout.html** – single logout template

### Recommendation:

Adapt \*.html files for production configuration to match the look and feel of the protected application improves user experience.

 © 2015 SWITCH

## Shibboleth2.xml Structure

44

Since Shibboleth 2.4: Simplified configuration but old format still accepted

<SPConfig> Document root element

Outer elements of the shibboleth.xml configuration file

|                                    |   |
|------------------------------------|---|
| <OutOfProcess> / <InProcess>       | (Optional) Log settings, extensions               |
| <UnixListener> / <TCPLListener>    | (Optional) Communication shibd/mod_shib           |
| <StorageService>                   | (Optional) Where session information is stored    |
| <SessionCache>                     | (Optional) Session timeouts and cleanup intervals |
| <ReplayCache>                      | (Optional) Where replay cache is stored           |
| <ArtifactMap>                      | (Optional) Timeout of artifact messages           |
| <RequestMapper>                    | (Optional) Session initiation and access control  |
| <b>&lt;ApplicationDefaults&gt;</b> | <b>Contains the most important settings of SP</b> |
| <SecurityPolicyProvider>           | Define various security options                   |
| <ProtocolProviders>                | Defines supported protocols (SAML, ADFS, ...)     |

## ApplicationDefaults Structure

45

You are most likely to modify <ApplicationDefaults>:

|                       |  |
|-----------------------|--|
| <Sessions>            | Defines handlers and how sessions are initiated and managed. Contains <SSO>, <Logout>, <Handler> |
| <Errors>              | Used to display error messages. E.g. logo, email and CSS   |
| <RelyingParty>        | (optional) To modify settings for certain IdPs/federations                                       |
| <MetadataProvider>    | Defines the metadata to be used by the SP  |
| <AttributeExtractor>  | Attribute map file to use  |
| <AttributeResolver>   | Attribute resolver file to use   |
| <AttributeFilter>     | Attribute filter file to use   |
| <CredentialResolver>  | Defines certificate and private key to be use  |
| <ApplicationOverride> | <b>(Optional) Can override any of the above for certain applications</b>                         |

## File Editing Commands for Terminal Editor

46

| Editor            | nano                                       | vim  |
|-------------------|--|--|
| Open file         | <code>\$ nano &lt;file&gt;</code>          | <code>\$ vim &lt;file&gt;</code>                             |
| Save file         | <code>&lt;ctrl&gt;-o</code>                | <code>&lt;esc&gt;, :w</code>                                 |
| Save and exit     | <code>&lt;ctrl&gt;-x</code>                | <code>&lt;esc&gt;, :wq</code>                                |
| Search string     | <code>&lt;ctrl&gt;-w, <b>string</b></code> | <code>&lt;esc&gt;, /<b>string</b></code>                     |
| Go to line number | <code>&lt;ctrl&gt;--, <b>number</b></code> | <code>&lt;esc&gt;, <b>number</b>,<br/>&lt;shift&gt;-G</code> |

**gedit** is the recommended text editor. Is started as root user. Its icon is in the launch bar on the left side of the desktop.



## Debugging SP Problems on Linux

47

1. Make sure the edited XML config file is valid and correct XML with:

```
$ xmlwf /etc/shibboleth/shibboleth2.xml
$ sudo shibd -t or
$ sudo shibd -tc /etc/shibboleth/shibboleth2.xml
```

2. Stop Shibboleth daemon with:

```
$ /etc/init.d/shibd stop
```

3. Increase log verbosity of shibd by seting log level to DEBUG in:

```
/etc/shibboleth/shibd.logger
```

4. Have a look at log file and search ERROR or CRIT messages in:

```
$ tail -f /var/log/shibboleth/shibd.log
```

5. Start Shibboleth daemon again with:

```
$ /etc/init.d/shibd start
```

6. If you fixed an error, also restart Apache with:

```
$ /etc/init.d/apache2 restart
```

Don't forget to set log level back to `INFO` for a production service



## Debugging SP Problems on Windows

48

1. Make sure the edited XML config file is valid XML by opening in Firefox the Shibboleth configuration file:  
`C:\opt\shibboleth-sp\etc\shibboleth\shibboleth2.xml`  
Firefox checks if XML file is well-formed
2. Check Shibboleth configuration file:  
`$ C:\opt\shibboleth-sp\sbin\shibd.exe -check`
3. Stop “Shibboleth 2 Daemon” in Windows Services
4. Increase log verbosity of shibd by setting log level to DEBUG in  
`C:\opt\shibboleth-sp\etc\shibboleth\shibd.logger`
5. Have a look at log file and search for ERROR and CRIT messages in:  
`C:\opt\shibboleth-sp\var\log\shibboleth\shibd.log`
6. Start “Shibboleth 2 Daemon” in Windows “Services” again
7. If the error is fixed, also restart Apache or IIS in Windows Services  
Don't forget to set log level back to `INFO` for a production service



## Logging

49

- Your number one friend in case of problems
- `shibd.log` and `transaction.log` written by shibd,  
`native.log` written by mod\_shib
- `*.logger` files contain predefined settings for output locations and a default logging level (`INFO`) along with useful categories to raise to `DEBUG`



## Increase Log Level to DEBUG

 50

- Raise categories:

```
$ vim /etc/shibboleth/shibd.logger
```

Line 2:

```
log4j.rootCategory=DEBUG, shibd_log, warn_log
```

Line 16:

```
# tracing of SAML messages and security policies
log4j.category.OpenSAML.MessageDecoder=DEBUG
log4j.category.OpenSAML.MessageEncoder=DEBUG
log4j.category.OpenSAML.SecurityPolicyRule=DEBUG
```

## Make Session Handler Show Values

 51

- For debugging purposes, it helps seeing the attribute values on /Shibboleth.sso/Session

- Open the /etc/shibboleth/shibboleth2.xml

```
$ vim /etc/shibboleth/shibd.logger
```

Line 53:

```
<!-- Session diagnostic service. -->
<Handler type="Session"
    showAttributeValues="true"
    Location="/Session"/>
```

## Apply Configuration Changes

 52

- To follow the shibd log file in real time and examine what happens during a login use tail (not available on Windows):

```
$ tail -f /var/log/shibboleth/shibd.log
```

- shibd reloads configuration when shibboleth2.xml is changed, but generally it is still better to restart shibd:

```
$ /etc/init.d/shibd restart
```

Shibboleth detects invalid configurations if it reloads them automatically. In this case it will continue to use the last valid configuration it still has in memory.

This behavior hides errors that will only be discovered at the next restart!

 © 2015 SWITCH

## Check Changes

 53

Login again with:

<https://sp#.example.org/Shibboleth.sso/Login>

You should see the encrypted and decrypted XML assertion received by SP

```
DEBUG Shibboleth.SSO.SAML2 [1]: decrypted Assertion: <saml2:Assertion
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_efc943c04c742ae96d15e19e95afba68"
IssueInstant="2014-02-10T14:59:29.841Z" Versi
on="2.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">[...]
```

And the Session Handler should now display also the attribute values:

```
Attributes
affiliation: faculty
eduPersonPrincipalName: 23489ch-234c89y32u@example.org
givenName: Giovanni
homeOrganization: aai-demo-idp.switch.ch
homeOrganizationType: others
mail: g.utente@example.org
```

 © 2015 SWITCH

- Metadata describes the other components (IdPs) that the Service Provider can communicate with
- **Four primary methods built-in:**
  - **Local metadata file (you download/edit it manually)**
  - **Downloaded remotely from URL (periodic refresh, local backup)**
  - Dynamic resolution of entityID (=URL), hardly used
  - "Null" source that disables security ("OpenID" model), hardly used
- Security comes from metadata filtering, either by you or the SP:
  - Signature verification
  - Expiration dates
  - White and blacklists

## Signature Verification

- Have a look at the configuration :

```
$ vim /etc/shibboleth/shibboleth2.xml
```

Change the certificate of MetadataProvider signature verification:

Line 72:

```
<MetadataProvider type="XML" [...] >  
  <MetadataFilter type="Signature" [...]  
    <TrustEngine type="StaticPKIX"  
      certificate="sp-cert.pem"  
      [...]  
    </TrustEngine>  
  </MetadataProvider>
```

- Then go to next slide...

## Signature Verification Continued



Run `$ shibd -tc /etc/shibboleth/shibboleth2.xml`

Output should look like:

```
ERROR OpenSSL : path validation failure at depth(2): self signed
certificate in certificate chain
ERROR OpenSSL : path validation failure at depth(2): self signed
certificate in certificate chain
WARN OpenSAML.MetadataFilter.Signature : filtering out group at root of
instance after failed signature check: TrustEngine unable to verify
signature.
CRIT Shibboleth.Application : error initializing MetadataProvider:
SignatureMetadataFilter unable to verify signature at root of metadata
instance.
overall configuration is loadable, check console for non-fatal problems
```

Metadata could not be loaded because it was signed with a different key (we "broke" the setup). So, let's get the right key...



## Signature Verification Corrected again



- To correct the metadata signature validation again :

```
$ vim /etc/shibboleth/shibboleth2.xml
```

Change the certificate of MetadataProvider signature verification:

Line 72:

```
<MetadataProvider type="XML" [...] >
  <MetadataFilter type="Signature" [...]
    <TrustEngine type="StaticPKIX"
      certificate="SWITCHaaiRootCA.crt.pem"
    [...]
  </MetadataProvider>
```

- Then restart shibd and try logging in again to check if metadata is accepted again



<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMetadataFilter>



## Skip Discovery Service

 58

- Discovery Service/WAYF can be skipped if service has only users from one organisation.

```
$ vim /etc/shibboleth/shibboleth2.xml
```

Change the SSO element to look like below to send users directly to the AAI Demo Home Organisation for authentication:

Line 34:

```
<SSO
    entityID="https://aai-demo-idp.switch.ch/idp/shibboleth">
SAML2
</SSO>
```

- Then again access `/Shibboleth.sso/Login`  
You should now directly be sent to login page of Demo IdP

## Discovery Service Options

59

What Discovery Service implementations are there? What are the advantages and considerations?



Please consult the table of contents to find this presentation in your hand-outs.

### Goals:

1. Learn how attributes are mapped and filtered
2. See how attributes can be used as identifiers
3. Add an attribute mapping and filtering rule

## Attribute Mappings

- SAML attributes from any source are "extracted" using the configuration rules in attribute map file in:  
`/etc/shibboleth/attribute-map.xml`
- Each element is a rule for decoding a SAML attribute and assigning it a local `id` which becomes its mapped variable name
- Attributes can have one or more `id` and multiple attributes can be mapped to the same `id`
- The `id` is also used as header name in the webserver for this attribute.

## Dissecting an Advanced Attribute Rule

 62

Line 139 (attribute-map.xml):

```
<Attribute
  name="urn:mace:dir:attribute-def:eduPersonScopedAffiliation"
  id="scoped-affiliation" >
  <AttributeDecoder xsi:type="ScopedAttributeDecoder"
    caseSensitive="false"/>
</Attribute>
```

- **name**  
SAML attribute name or NameID format to map from
- **id**  
The primary "id" to map into, also used in web server environment
- **AttributeDecoder xsi:type**  
Decoder plugin to use (defaults to simple/string)
- **caseSensitive**  
How to compare values at runtime (defaults to true)

## Adding Attribute Mappings

 63

- Add eduPersonPrincipal name SAML 2 attribute mappings:

```
$ vim /etc/shibboleth/attribute-map.xml
```

Line 18:

```
<Attribute
  name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
  id="eduPersonPrincipalName" />
```

- After saving, changes take effect immediately but NOT for any existing sessions
- Therefore, restart your browser (or delete your session cookies) and continue on next slide ...

## Testing Added Attribute Mapping

 64

- Then access `/Shibboleth.sso/Login` and log in again.
- After that, check the Shibboleth Session Handler  
You should now also see the `eduPersonPrincipalName`

```
Attributes
affiliation: faculty
eduPersonPrincipalName: 23489ch-234c89y32u@example.org
entitlement: http://example.org/res/99999;http://publisher-xy.com/e-journals
givenName: Giovanni
homeOrganization: aai-demo-idp.switch.ch
homeOrganizationType: others
mail: g.utente@example.org
```

## Side note: Aliases

65

- The `attribute-map.xml` supported attribute aliases like:

```
<Attribute id="Shib-EP-Affiliation"
  name="urn:mace:dir:attribute-def:eduPersonAffiliation"
  aliases="affiliation aff affil" />
```

- Allowed using aliases in access control rules like:  
`require affiliation staff`  
`require Shib-EP-Affiliation staff`
- Aliases are deprecated since 2.5
- Recommend to use only official LDAP names in the future  
(e.g. `surname`, `givenName`, `mail`)

## Attribute Filtering

- Answers the "who can say what" question on behalf of an application
- Service Provider can make sure that only allowed attributes and values are made available to application
- Some examples:
  - constraining the possible values or value ranges of an attribute (e.g. eduPersonAffiliation, telephoneNumber, ....)
  - limiting the scopes/domains an IdP can speak for (e.g. university x cannot assert faculty@university-z.edu)
  - limiting custom attributes to particular sources

## Default Filter Policy

- As default, **attributes are filtered out unless there is a rule!**
- Shared rule for legal affiliation values
- Shared rule for scoped attributes
- Generic policy applying those rules and letting all other attributes through
- Check `/var/log/shibboleth/shibd.log` for signs of filtering in case of problems with attributes not being available. You would find something like "no values left, removing attribute (#attribute name#)"

## Add a Source-Based Filtering Rule

 68

- Add a rule to limit acceptance of "sn" to a single IdP:

```
$ vim /etc/shibboleth/attribute-policy.xml
```

Add surname mapping **and** comment out catch-all rule at bottom :

Line 145:

```
<afp:AttributeRule attributeID="surname">
  <afp:PermitValueRule
    xsi:type="AttributeIssuerString"
    value="https://aai-demo-idp.switch.ch/idp/shibboleth"/>
</afp:AttributeRule>
<!--
<afp:AttributeRule attributeID="*>
  <afp:PermitValueRule xsi:type="ANY"/>
</afp:AttributeRule>
-->
```

After login: **givenName** is filtered out but **surname** is not due to rule



© 2015 SWITCH

<https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAddAttributeFilter>

## Add Catch-all Rule Again

 69

- Add a rule to limit acceptance of "sn" to a single IdP:

```
$ vim /etc/shibboleth/attribute-policy.xml
```

Line 145:

```
<afp:AttributeRule attributeID="surname">
  <afp:PermitValueRule xsi:type="AttributeIssuerString"
    value="https://non.existing.example.org/idp/shibboleth"/>
</afp:AttributeRule>
```

Uncomment catch-all rule at bottom:

```
<afp:AttributeRule attributeID="*>
  <afp:PermitValueRule xsi:type="ANY"/>
</afp:AttributeRule>
```

Then login again: surname is now filtered out but other attributes aren't.

Because a specific rule exists, the catch-all rule does not apply anymore!



© 2015 SWITCH

## Remove Specific Rule

 70

- Remove rule for (non-) acceptance of `surname`:

```
$ vim /etc/shibboleth/attribute-policy.xml
```

Delete rule for `surname` again.

- Save file and access `/Shibboleth.sso/Login` again
- Now you should see the `surname` attribute again

## Interfederation Attributes and Checking

71

Excursion about user attributes available via AAI.



Please consult the table of contents to find this presentation in your hand-outs.

### Goals:

1. Learn how to initiate a Shibboleth session
2. Understand their advantages/disadvantages
3. Know where to require a session, what to protect

- Before access control (will be covered later on) can occur, a Shibboleth session must be initiated
- Session Initiation and content protection go hand in hand
- Requiring a session means the user has to authenticate
- Only authenticated users can access protected content



## Content Protection Settings

 74

Protect hosts, directories, files or queries

- **Apache**  
.htaccess (dynamic) or httpd.conf (static)
- **Apache / IIS / other**  
<RequestMap> in shibboleth2.xml  
Requires Shibboleth to know exact hostname  
Very powerful and flexible thanks to boolean/regex operations
- Try accessing `https://sp#.example.org/secure/`  
You should get access because the directory is not protected (yet)  
`/secure/` used to be protected by default in older Shibboleth distributions

## Content Protection with .htaccess File

 75

- Let's protect the directory by requiring a Shibboleth session:

```
$ vim /var/www/secure/.htaccess
```

```
AuthType shibboleth
require shibboleth
ShibRequestSetting requireSession true
```

Synonym for the last line (used in Shibboleth 1.3, deprecated):

```
ShibRequireSession On
```

Rules could also be in static httpd configuration file directly, see

`/etc/apache2/conf.d/shib.conf` ( default rule for `/secure/` )

## Session Initiation and Content Settings

76

- **forceAuthn** (`ShibRequestSetting forceAuthn true`)
  - Disable Single-Sign on and force a re-authentication
- **isPassive** (`ShibRequestSetting isPassive true`)
  - Check whether a user has an SSO session and if he has, automatically create a session on SP without any user interaction
- Use a specific IdP to use for authentication
- Requesting types of authentication
  - E.g enforce X.509 user certificate authentication
- Custom error handling pages to use
- Redirection-based error handling
  - In case of an error, redirect user to custom error web page with error message/type as GET arguments

## Test Content Protection Rule

 77

- Clear session and then access the protected URL again:  
`https://sp#.example.org/secure`
- Authentication is enforced and access should be granted
- Currently, all authenticated users get access
- Content protection to limit access only to specific users will be covered later

## Content Protection with RequestMap

 78

- `mod_shib` provides request URL to `shibd` to process it  
Therefore, `shibd` can enforce access control as well  
**This is required for IIS web servers!**
- First ensure that requests for `/other-secure/` are handled by `shibd` without setting any specific session requirements:

```
$ vim /var/www/other-secure/.htaccess
```

```
AuthType shibboleth  
require shibboleth
```

## How to Add a RequestMap

 79

- Open the Shibboleth configuration:

```
$ vim /etc/shibboleth/shibboleth2.xml
```

Before `<ApplicationDefaults>` insert a `<RequestMap>`:

Line 7:

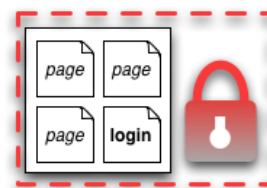
```
<RequestMapper type="Native">  
  <RequestMap applicationId="default">  
    <Host name="sp#.example.org">  
      <Path name="other-secure"  
        authType="shibboleth" requireSession="true"/>  
    </Host>  
  </RequestMap>  
</RequestMapper>
```

- Clearing session and then accessing `/other-secure/` now, one also is forced to authenticate

## Where to Require a Shibboleth Session

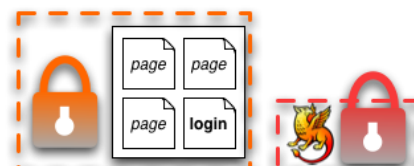
- **Whole application with "required" Shibboleth session**

- Easiest way to protect a set of documents
- No other authentication methods possible
- Needs special config to preserve HTTP POST requests



- **Whole application with "lazy" Shibboleth session**

- Also allows for other authentication methods
- Authorization can only be done in application



- **Only page that sets up application session**

- Well-suited for dual login
- Application can control session time-out
- **Generally the most popular solution (many Shibboleth-enabled applications use this)**



## Protect a Simple Web Application

- **Access** `https://sp#.example.org/cgi-bin/attribute-viewer` Simple CGI script as a sample application that show attributes.

- Lets protect that script with Shibboleth by requiring a session:

```
$ vim /usr/lib/cgi-bin/.htaccess
```

```
AuthType shibboleth
ShibRequestSetting requireSession true
require shibboleth
```

This will require a session for all requests to `/cgi-bin/` and make attributes available to application in environment.

- Try again to access script with a browser:  
Script should enforce authentication and show attributes

## Make Script "see" Shibboleth Session

 82

- What if we wanted to grant access also to non-authenticated users but use attributes if somebody is authenticated?
- Use Shibboleth (lazy) session:

```
$ vim /usr/lib/cgi-bin/.htaccess
```

```
AuthType shibboleth  
require shibboleth
```

This will not require a session but make attributes available to application in environment if somebody has a session.

- Try again with a browser:

```
https://sp#.example.org/cgi-bin/attribute-viewer
```

Unauthenticated access still possible. No attributes are shown yet.

## REMOTE\_USER

83

- Special single-valued variable that all web applications should support for container-managed authentication of a unique user.
- Any attribute, once extracted/mapped, can be copied to REMOTE\_USER
- Multiple attributes can be examined in order of preference, but only the first value will be used.

## Changing REMOTE\_USER

 84


- In case your application needs to have a remote user for authentication, you just could make shibboleth put an attribute (e.g. "mail") as REMOTE\_USER:

```
/etc/shibboleth/shibboleth2.xml
```

Line 12 in <ApplicationDefaults>:

```
REMOTE_USER="mail eppn persistent-id targeted-id"
```

- If mail attribute is available, it will be put into REMOTE\_USER
- Attribute `mail` has precedence over `persistent-id` in this case
- This allows very easy "shibbolization" of some web applications

 © 2015 SWITCH

## How To Initiate a (Lazy) Session

 85

- Close your browser, and access the attribute-viewer again,  
`https://sp#.example.org/cgi-bin/attribute-viewer`
- Then click on one of the buttons and login at Test IdP  
You should be sent to IdP or WAYF and attribute-viewer should display attributes after successful authentication
- Have a look at the HTML source and what it does:  
`https://sp#.example.org/cgi-bin/attribute-viewer`
- Script initiates Shibboleth session by sending user to:  
`/Shibboleth.sso/Login?target=/cgi-bin/attribute-viewer  
&entityID=https://aai-demo-idp.switch.ch/idp/shibboleth`

 © 2015 SWITCH

## Try to Initiate a Session Yourself

 86


- Try to construct a Session Initiation URL yourself by using these parameters to see the result: e.g. try supplying the IdP:  
`https://sp#.example.org/Shibboleth.sso/Login?  
target=https://sp#.example.org/cgi-bin/attribute-viewer&  
entityID=https://aai-demo-idp.switch.ch/idp/shibboleth`
- This way, a session using a specific IdP can be initiated directly with a link, e.g. on a portal web page.
- This allows creating "login links" to skip the WAYF/Discovery Service
- It also allows overriding certain content settings

 © 2015 SWITCH

## Session Creation Parameters

87

- Key Parameters
  - `target` (defaults to `homeURL` or `"/"`)
  - `entityID` (specific IdP to use or WAYF/DS if not present)
- Most parameters can be set at three places.  
In order of precedence:
  - In query string parameter of a URL to handler
  - a content setting (`.htaccess` or `RequestMap`)
  - `<SessionInitiator>` element

 © 2015 SWITCH <https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessionCreationParameters>

## Lazy Sessions Summary

88

- Won't enforce a Shibboleth session but use it if it is available
  - If valid **session exists**
    - then process it as usual (put attributes in server environment, etc.), but if a **session does NOT exist** or is invalid,
      - ignore it and pass on control to application
- Three common cases:
  - Public and private access to the same resources
  - Separation of application and SP session
  - Dual login (use Shibboleth and some other authentication method)

## Using Lazy Sessions

89


- In place of an API to "doLogin", the SP uses redirects:  
`https://testsp1.example.org/Shibboleth.sso/Login`
- When your application wants a login to happen, redirect the browser to a SessionInitiator (`/Shibboleth.sso/Login` by convention) with any parameters you want to supply



## Some Concerns Regarding Dual Login

90

- Can be a viable option in case application must also be accessed by non-Shibboleth users
- Generally not recommended due to issues with:
  - **Usability:** Difficult to teach the users how to authenticate
  - **Security:** Shibboleth users shouldn't enter their password in the login form for the non-Shibboleth users...

|  |  |
|--|--|
| <br><a href="#">About AAI</a> : <a href="#">FAQ</a> : <a href="#">Help</a> : <a href="#">Privacy</a><br><br><b>Login for AAI users</b><br>Login service for members of the<br><a href="#">SWITCHaai Federation participants</a> .<br><br><input type="button" value="Login"/> | <b>Login for non-AAI users</b><br>Username:<br><input type="text"/><br>Password:<br><input type="password"/><br><br><input type="button" value="Login"/> |
|--|--|

## Access Control

91

### Goals:

1. Create some simple access control rules
2. Get an overview about the three ways to authorize users
3. Understand their advantages/disadvantages

- Integrated in Service Provider via an AccessControl API built into the request processing flow
- Two implementations are provided by the SP:
  - .htaccess "require" rule processing
  - XML-based policy syntax attached to content via RequestMap
- Third option: Integrate access control into web application

## Access Control Mechanisms

|   | 1.a httpd.conf  | 1.b .htaccess  | 2. XML AccessControl *   | 3. Application Access Control  |
|---|---|--|--|--|
| ⊕ | <ul style="list-style-type: none"> <li>■ Easy to configure</li> <li>■ Can also protect locations or virtual files</li> <li>■ URL regex</li> </ul> | <ul style="list-style-type: none"> <li>■ Dynamic</li> <li>■ Easy to configure</li> </ul>   | <ul style="list-style-type: none"> <li>■ Platform independent</li> <li>■ Powerful boolean rules</li> <li>■ URL Regex</li> <li>■ Dynamic</li> </ul> | <ul style="list-style-type: none"> <li>■ Very flexible and powerful with arbitrarily complex rules</li> <li>■ URL Regex Support</li> </ul> |
| ⊖ | <ul style="list-style-type: none"> <li>■ Only works for Apache</li> <li>■ Not dynamic</li> <li>■ Very limited rules</li> </ul>                    | <ul style="list-style-type: none"> <li>■ Only works for Apache</li> <li>■ Only usable with "real" files and directories</li> </ul> | <ul style="list-style-type: none"> <li>■ XML editing</li> <li>■ Configuration error can prevent SP from restarting</li> </ul>                      | <ul style="list-style-type: none"> <li>■ You have to implement it yourself</li> <li>■ You have to maintain it yourself</li> </ul>          |

\* Configured in RequestMap or referenced by an .htaccess file

## 1. Apache httpd.conf or .htaccess Files

- Work almost like known Apache "require" rules  
E.g `Require shib-attr affiliation staff`  
or `Require shib-attr mail user1@idp1.com user2@idp2.org`
- Special rules:
  - `shibboleth` (no authorization)
  - `valid-user` (require a session, but NOT identity)
  - `user` (REMOTE\_USER as usual)
  - `authnContextClassRef`, `authnContextDeclRef`
- Default is boolean "OR", use `ShibRequireAll` for AND rule
- Regular expressions supported using special syntax:  
`Require shib-attr mail ~ [exp]`  
`Require shib-attr mail ~ ^.*@(it|faculty).example.org$`

## 1. Example .htaccess File

- Require a user to be a staff member:

```
$ vim /var/www/staff-only/.htaccess
```

```
AuthType shibboleth
ShibRequestSetting requireSession true
Require shib-attr affiliation staff
```

Then access: `https://sp#.example.org/staff-only/`  
with `h.mitarbeiter/password`. Access should be granted.

- Then try the same again with `p.etudiant/password`  
Access should be denied



## 1. More Advanced .htaccess File

- Require a user to be a student or to have an entitlement:

```
$ vim /var/www/students-only/.htaccess
```

```
AuthType shibboleth
ShibRequestSetting requireSession 1
require affiliation student
require entitlement ~ .*example\.org.*
```

Then access : `https://sp#.example.org/students-only/`  
with `p.etudiant/password`. Access should be granted.

- Then try the same with `h.mitarbeiter/password`  
Access should be granted too because this staff member has entitlement!



## 2. XML Access Control

- Can be used for access control independent from web server and operating system
- XML Access control rules can be embedded inside RequestMap or be dynamically loaded from external file
- Boolean operators (AND,OR,NOT) can be used
- .htaccess files can reference to XMLAccessControl files  
Allows outsourcing access control rules to non-root users





## 2. XML Access Control Example

- Require an entitlement or specific users (same as before):

```
$ vim /etc/shibboleth/shibboleth2.xml
```

Line 8:

```
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="sp#.example.org">
      <Path name="other-secure" authType="shibboleth" requireSession="true" />
      <Path name="cgi-bin" authType="shibboleth" requireSession="true">
        <AccessControl>
          <OR>
            <RuleRegex require="entitlement">^.*agreement.*$ </RuleRegex>
            <Rule require="affiliation">student</Rule>
          </OR>
        </AccessControl>
      </Path>
    </Host>
  </RequestMap>
</RequestMapper>
```

- Access** `https://sp#.example.org/cgi-bin/attribute-viewer`  
Once with `h.mitarbeiter` (access denied) and `p.etudiant` (access granted)



© 2015 SWITCH

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPXMLAccessControl>

## 3. Application Managed Access Control

- Application can access and use Shibboleth attributes by reading them from the web server environment
- Attributes then can be used for authentication/access control/authorization

### PHP:

```
if ($_SERVER['affiliation'] == 'staff;member')
{ grantAccess() }
```

### Perl:

```
if ($ENV{'affiliation'} == 'staff;member')
{ &grantAccess() }
```

### Java:

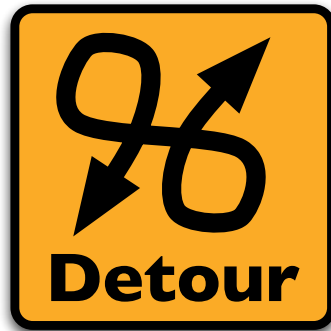
```
if (request.getHeader("affiliation").equals("staff;member") )
{ grantAccess() }
```



© 2015 SWITCH

## SWITCHtoolbox and Group Management Tool 100

Excursion about using the Group Management Tool (GMT) or the SWITCHtoolbox.



Please consult the table of contents to find this presentation in your hand-outs.

## Using the SWITCHaai Embedded WAYF 101

### Goals:

1. Add the Embedded WAYF to a HTML web page
2. Configure Embedded WAFY
3. Add the Guest Login IdP to the Embedded WAYF
4. Configure discovery for a single IdP

## How to Add Embedded WAYF

- Open in Web Browser (login with your AAI Account):  
[https://rr.aai.switch.ch/gen\\_embedding\\_code.php](https://rr.aai.switch.ch/gen_embedding_code.php)  
Then type `sp#.example.org` and select your SP
- Or without AAI Login:  
<https://wayf-test.switch.ch/SWITCHaai/WAYF/embedded-wayf.js/snippet.html>
- Copy the whole HTML snippet
- Then open `/var/www/index.html` in  

```
$ vim /var/www/index.html
```

  
and paste the snippet after line 24  

```
<!-- EMBEDDED-WAYF-START -->
<script type="text/javascript"><!--

// To use this JavaScript, please access:
[...]
```

## Configure Embedded WAYF

- Adapt essential settings of Embedded WAYF

```
$ vim /var/www/index.html
```

Edit the following mandatory settings of the Embedded WAYF

```
// EntityID of the Service Provider that protects this Resource
[...]
var wayf_sp_entityID = "https://sp#.example.org/shibboleth";

// Shibboleth Service Provider handler URL
[...]
var wayf_sp_handlerURL = "https://sp#.example.org/Shibboleth.sso";

// URL on this resource that the user shall be
[...]
var wayf_return_url = "https://sp#.example.org/cgi-bin/attribute-viewer";
```

## Test the Embedded WAYF

- Access the URL `https://sp#.example.org/`
- Select the Test Identity Provider in the drop-down list
- Authenticate with demostudent/demo  
You should see access to the attribute-viewer
  
- Go back to `https://sp#.example.org/`  
Note how the Embedded WAYF now looks different
  
- Set `var wayf_auto_redirect_if_logged_in = true;`  
and open again `https://sp#.example.org/`

## Configure discovery for a single IdP

Configure your SP to use only a specific IdP (demo-idp or guest-login) and skip the Discovery Service/WAYF:

```
<SSO entityID="https://aai-demo-idp.switch.ch/idp/shibboleth">
    SAML2
</SSO>
```

or

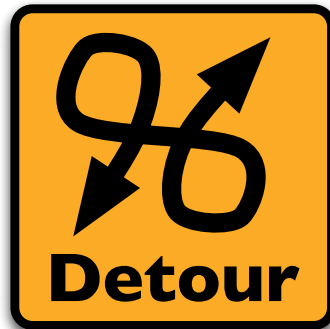
```
<SSO entityID="https://aai.guest-login.ch/idp/shibboleth">
    SAML2
</SSO>
```

Test the configuration:

```
$ shibd -tc /etc/shibboleth/shibboleth2.xml
```



What is possible and what are the limitations of local and global logout.



Please consult the table of contents to find this presentation in your hand-outs.

How to protect multiple applications with one physical Service Provider and how to have one Shibboleth application distributed across multiple physical hosts.



Please consult the table of contents to find this presentation in your hand-outs.

### Goals:

1. Understand the idea of a handler
2. Get an overview about the different types of handlers
3. Know how to configure them if necessary

## SP Handlers

### ■ "Virtual" applications inside the SP with API access:

- SessionInitiator (requests)  
Start Shibboleth session: `/Shibboleth.sso/Login`
- AssertionConsumerService (incoming SSO)  
Receives SAML assertions: `/Shibboleth.sso/SAML/POST`
- LogoutInitiator (SP signout)  
Log out from SP: `/Shibboleth.sso/Logout`
- SingleLogoutService (incoming SLO)
- ManageNameIDService (advanced SAML)
- ArtifactResolutionService (advanced SAML)
- Generic (diagnostics, other useful features)
  - Returns session information: `/Shibboleth.sso/Session`
  - Returns detailed SP status: `/Shibboleth.sso/Status`
  - Returns SP metadata: `/Shibboleth.sso/Metadata`

- The URL of a handler = handlerURL + the Location of the handler.  
E.g. for a virtual host testsp.example.org with handlerURL of "/Shibboleth.sso", a handler with a Location of /Login will be `https://sp#.example.org/Shibboleth.sso/Login`
- Handlers aren't always SSL-only, but usually should be Recommended to set handlerSSL="true" in shibboleth2.xml
- Metadata basically consists of entityID, keys and handlers
- Handlers are never "protected" by the SP  
But sometimes by IP address (e.g. with `acl="127.0.0.1"`)

## Error Pages and Customization

How to improve the user experience by customizing error pages.

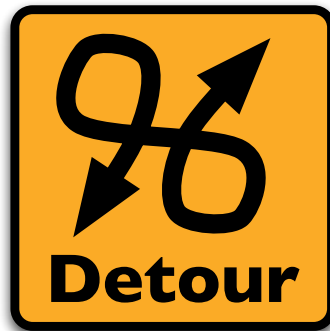


Please consult the table of contents to find this presentation in your hand-outs.


## Shibboleth-aware Applications

112

Some examples of applications that already support Shibboleth out of the box.



Please consult the table of contents to find this presentation in your hand-outs.

 © 2015 SWITCH

## Try Demo Yourself

To refresh how AAI Login works



# SWITCH

SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)

# Test AAI Login with Demo Service Provider



AAI Demo

SWITCH

↑ About AAI

Area: Any authenticated user

Shibboleth Service Provider, current <RequestMap />:

```
<Path
  name="secure"
  authType="shibboleth"
  requireSession="true">
</Path>
```

| Attributes  | Values   |
|---|--|
| <b>persistent-id</b><br>SAML2 Attribute Name:<br>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent | https://aai-login.example.org/ldap/shibboleth!https://aai-demo.switch.ch/shibboleth!iIRU39h9rzgVOi4FwyWFt2RvsN8= |
| <b>uniqueid</b><br>SAML2 Attribute Name:<br>urn:oid:2.16.756.1.2.5.1.1.1                              | 2490257@example.org  |
| <b>givenName</b><br>SAML2 Attribute Name:<br>urn:oid:2.5.4.42   | Test1  |
| <b>surname</b><br>SAML2 Attribute Name:   | Student  |

1. In Firefox, open [aai-demo.switch.ch](https://aai-demo.switch.ch)
2. Click on "Any authenticated user"
3. Select the "Example Organisation" (running on your VM)
4. Log in using a test user (e.g. "student1" "password1")

© 2015 SWITCH

2

## X.509 Certificates for SAML

Shibboleth and public-key cryptography



SWITCH

SWITCHaai Team  
aai@switch.ch

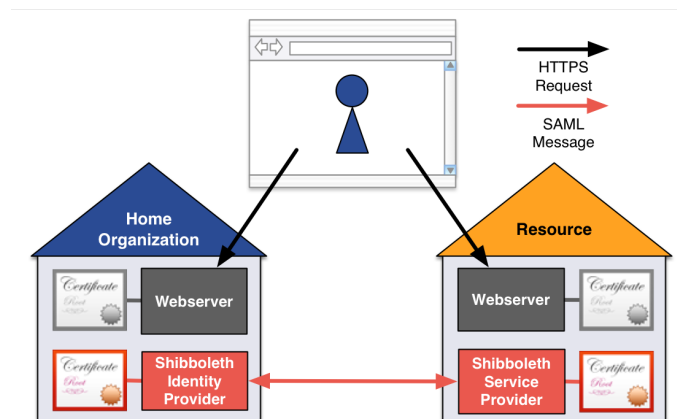
© SWITCH 2015

# IdP-to-SP communication

- To secure communications between an IdP and an SP (or vice versa), each entity needs a key pair:
  - for authenticating/signing SAML messages
  - for encrypting SAML messages
- The most popular public-key algorithm today is RSA, typically with a key size of 2048 bits
- X.509 is a standardized, ubiquitous format for public-key data structures, so it's convenient for use as a container for public keys in the SAML world

## X.509 certificates: a bird's eye view

- certificate = public key + name + signature
- the two “certificate worlds” of a Shibboleth SP (or IdP):
  - SSL/TLS between the user's browser and the Web server
  - XML Signature and XML Encryption for SAML messaging between the SP and the IdP



## X.509 certificate validation

- for SSL/TLS, validating the certificate's name and signature by the browser is absolutely crucial
  - browsers validate the chain against a built-in set of root certificates by verifying the signatures, and *must* make sure that the name is matching (would be vulnerable to MiTM otherwise)
- for the SAML world and the SWITCHaai federation, certificates are fully embedded in the federation metadata, and only the public key is considered by Shibboleth (X.509 is used as a convenient container format)
  - name and signature are basically thrown away

## SWITCHaai requirements for SAML embedded certificates

- *either* a self-signed certificate with minimal subject information and X.509v3 extensions (**recommended**, can be created with the `keygen` script bundled with the Shibboleth SP)
- *or* a certificate signed by a well-known CA, with organization validation (OV), chaining to a root trusted by either Microsoft or Mozilla
- further reading:
  - <https://www.switch.ch/aai/support/certificates/certificate-acceptance/>
  - <https://www.switch.ch/aai/support/certificates/embeddedcerts-requirements/>

# Examining X.509 certificates

- Details in text format:

```
openssl x509 -in /etc/ssl/certs/ssl-cert-snakeoil.pem -text
```

- Display the fingerprint only:

```
openssl x509 -in /etc/ssl/certs/ssl-cert-snakeoil.pem \
-noout -fingerprint [-sha256]
```

- Dump a pure Base64 block (e.g. when grabbing from XML metadata – paste into console and end with Ctrl-D):

```
openssl base64 -d | openssl x509 -inform der -text
```

## Discovery Service Options



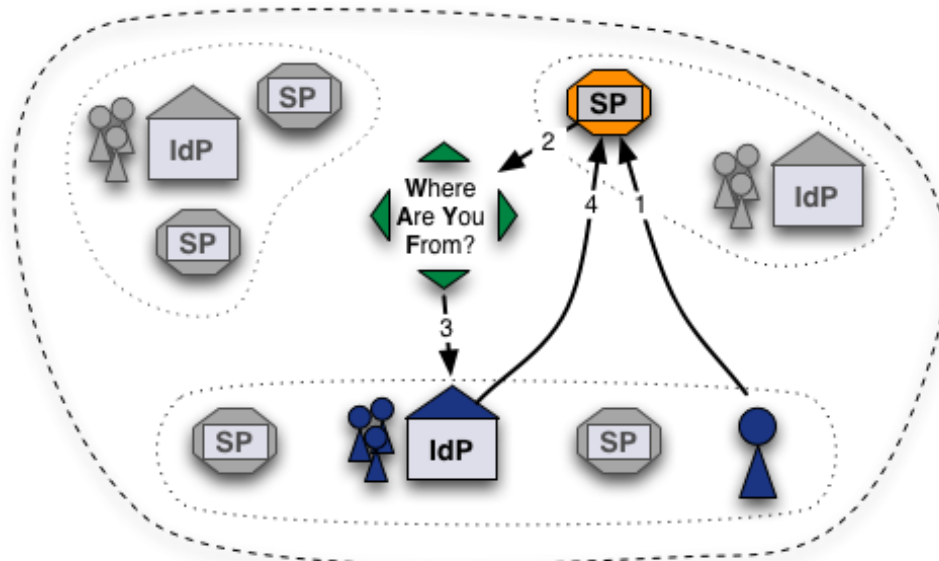
# SWITCH

SWITCHaai Team  
aai@switch.ch



## No Central WAYF for Interfederation

- The classic way: One WAYF per Federation



**WAYF achieves high availability through redundancy and IP Anycast.**

## Alternatives to Central WAYF

- Direct Login URLs
- SWITCH Embedded WAYF



- Shibboleth Embedded Discovery Service



## Solution 1: Direct Login URLs

- A separate login link for a specific IdP
- 1 click direct redirect to IdP without going via WAYF
- Useful when only users of few IdPs use resource

### Login links:

[Login via SWITCH \(SWITCHaai\)](#)

[Login via Munich University of Technology](#)

[Login via Eindhoven University of Technology](#)

## Composing Login URLs

### Required information

#### Service Provider Session Initiator Handler URL

Session Initiator ☒ /Login ☐ /DS

Since Shibboleth 2.5 the default Session Initiator is /Login, for older version you might have to use the /DS Session Initiator.

Enter the hostname of your SWITCHaai or AAI Test service and select one of the matching entries from the auto-completion feature.

Examples for valid Service Provider Session Initiator handler URLs are  
`https://myhost.example.com/Shibboleth.sso/Login` or  
`https://otherhost.example.com/Shibboleth.sso/DS`.

Service Provider Target URL

Specify here the URL of the web page that the user shall be redirected after authentication. This is usually a Shibboleth protected page. If you don't have such a page yet, use  
`https://your.example.com/Shibboleth.sso/Session` provided you are using a Service Provider 2.x.  
This page then will display all available attributes and other session information.

Identity Provider entityID

Enter the entityID of the Identity Provider. Examples are  
`https://aai-login.example.com`  
`https://aai.example.com`

☒ Service Provider ☐ Identity Provider

By default, the authentication process is initiated by the Service Provider. Identity Provider-initiated URLs work only with Shibboleth Identity Provider 2.3 or newer. They can be useful in specific use-cases but are generally not recommended to use.

## Solution 2: Embedded WAYF

### Bibliotheks-Ligin

**Bibliothekskunden**  
ausser Angehörige der ETH Zürich / EPF Lausanne

Benutzer- oder Ausweisnummer  Passwort

[Passwort vergessen?](#)  
[Neu registrieren](#)

Benutzerinnen und Benutzer mit einem in anderen [IDS-Verbünden](#) gültigen Benutzerausweis melden sich bitte mit ihrem üblichen Login an.


**Angehörige der ETH Zürich / EPF Lausanne**

[Passwort vergessen?](#)

OLAT login

Please select your university.

You will be redirected for authentication.



**SWITCHaai Login**

Studierende/ Mitarbeitende von Schweizer Hochschulen (ausser HFT und BFH-Externe):

Login with:

(Link)

Login Öbrige (einschl. HFT und BFH-Externe, nicht aai)

## Embedded WAYF

Enter the name of the organisation you are affiliated with...

**Last used**

- University of Basel
- EPFL - EPF Lausanne
- SWITCH

**Universities**

- EPFL - EPF Lausanne
- ETHZ - ETH Zurich
- Universita della Svizzera Italiana
- University of Basel
- University of Bern
- University of Fribourg
- University of Geneva
- University of Lausanne
- University of Liechtenstein
- University of Lucerne
- University of Neuchâtel
- University of St. Gallen
- University of Zurich

**University Hospitals**

- CHUV - University Hospital Lausanne
- HUG - Univ. Hospitals of Geneva
- Inselspital - University Hospital Bern
- University Hospital Zurich

**From other federations**

- Dalarna University
- Esslingen University of Applied Sciences

Zu

**Universities**

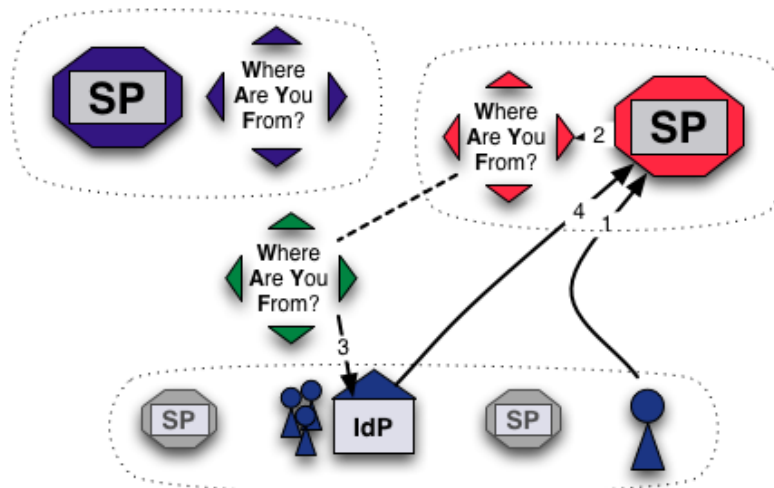
- ETHZ - ETH Zurich
- University of Zurich

**University Hospitals**

- University Hospital Zurich

## Embedded WAYF

- Embed WAYF on Web Application
- customize look and feel
- still transparently uses central WAYF



## Information and Configuration

More information about the Embedded WAYF:



<https://www.switch.ch/aai/guides/discovery/embedded-wayf/>

Generate the Embedded WAYF code for your SP:



[https://rr.aai.switch.ch/gen\\_embedding\\_code.php](https://rr.aai.switch.ch/gen_embedding_code.php)

## Configuration Example of Embedded WAYF

```
// Example of how to add Identity Provider from other federations
var wayf_additional_idps = [
    {name:"Esslingen University of Applied Sciences",
      entityID:"https://idp.hs-esslingen.de/idp/shibboleth",
      logoURL:"https://www2.hs-esslingen.de/favicon.ico"
    },
    {name:"Dalarna University",
      entityID:"https://login.du.se/idp/shibboleth",
      logoURL:"https://login.du.se/duse-logo-16x16.png"
    }
];
```

## Configuration (2)

## Configuration Example of Embedded WAYF

```
// EntityIDs of Identity Provider that should not be shown at all
// [Optional, commented out by default]

var wayf_hide_idps = new Array ("https://idemfero.units.it/idp/shibboleth",
  "https://idp.it.su.se/idp/shibboleth");

// Categories of Identity Provider that should not be shown
// Possible values
  are:"university","uas","hospital","library","vho","others","all"

var wayf_hide_categories = new Array("library","vho","others","hospital");
```

## Enable JSON Discovery feed to use local metadata of SP



In shibboleth2.xml:

```
<Sessions lifetime="28800"
    timeout="3600"
    relayState="ss:mem"
    checkAddress="false"
    consistentAddress="true"
    handlerSSL="true"
    cookieProps="https">
...
<!-- JSON feed of discovery information. -->
    <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>
</Sessions>
```

## JSON Discovery feed example



JSON result of an example discovery feed:  
<https://sp.example.org/Shibboleth.sso/DiscoFeed>

```
[
{ "entityID": "https://shibboleth-idp.uni-goettingen.de/uni/shibboleth",
  "DisplayNames": [
    { "value": "Georg-August Universität Göttingen", "lang": "de" },
    { "value": "Georg-August University Göttingen", "lang": "en" }
  ]
},
{ "entityID": "https://login.ntua.gr/idp/shibboleth",
  "DisplayNames": [
    { "value": "National Technical University of Athens", "lang": "en" },
    { "value": "Εθνικό Μετσόβιο Πολυτεχνείο", "lang": "el" }
  ]
},
]
```

## Configuration (3)

### Configuration Example of Embedded WAYF

```
// Whether to load Identity Providers from the Discovery Feed provided by
// the Service Provider.
// IdPs that are not listed in the Discovery Feed and that the SP therefore is
// not able to accept assertions from, are hidden by the Embedded WAYF
// IdPs that are in the Discovery Feed but are unknown to the SWITCHwayf
// are added to the wayf_additional_idps.
// The list wayf_additional_idps will be sorted alphabetically
// The SP must have configured the discovery feed handler that generates a
// JSON object. Otherwise it won't generate the JSON data containing the IdPs.
// [Optional, default:false]
```

```
var wayf_use_disco_feed = true;
```

## MetadataFilter Example

In shibboleth2.xml:

```
<MetadataProvider type="XML" .....>

  <MetadataFilter type="Whitelist">
    <Include>https://idp.nordu.net/idp/shibboleth</Include>
    <Include>https://idp.ids-mannheim.de/idp/shibboleth</Include>
    <Include>https://shibboleth.fhwn.ac.at/idp/shibboleth</Include>
    <Include>https://idp.it.su.se/idp/shibboleth</Include>
    <Include>https://tumidp.lrz.de/idp/shibboleth</Include>
  </MetadataFilter>

</MetadataProvider>
```

## Solution 3: Embedded Discovery Service



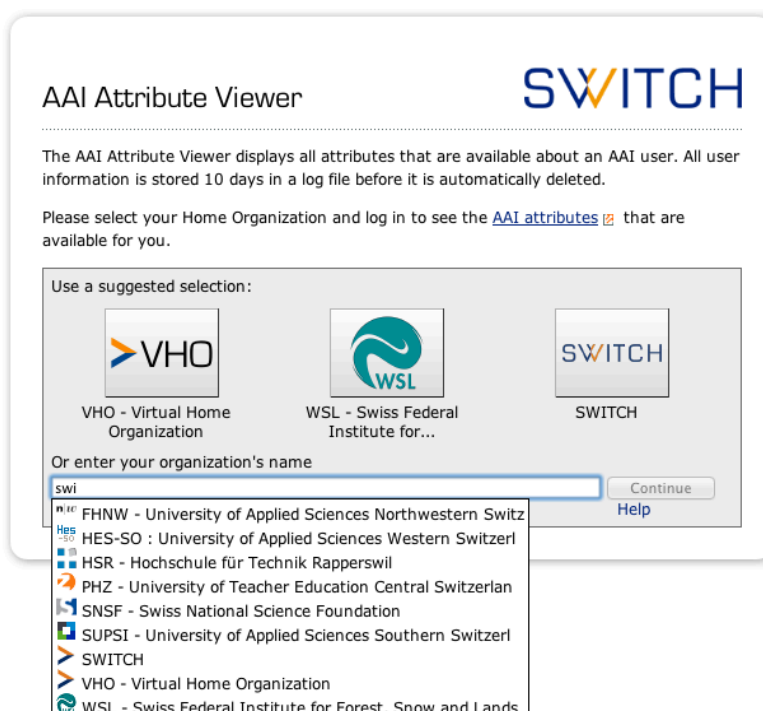
- Requires the Discovery Feed provided by the SP
- Embed the DS directly into the service
- Search-as-you-type or select from list
- JavaScript, CSS and HTML only
- developed and maintained by the Shibboleth team
- download from

 <https://shibboleth.net/downloads/embedded-discovery-service/latest/>

- Documentation can be found at:


 <https://wiki.shibboleth.net/confluence/display/EDS10/Embedded+Discovery+Service>

## Embedded Discovery Service






## Embedded WAYF vs Embedded DS

| Properties   | Login Link | Embedded WAYF<br>SWITCH | EDS<br> Shibboleth. |
|--|------------|-------------------------|--|
| Independent from central server                            | ✓          |                         | ✓  |
| Display only “valid” IdPs for SP                           |            | (✓)                     | ✓  |
| Search as you type feature                                 |            | ✓                       | ✓  |
| Show Home Org Logo   | (✓)        | ✓                       | ✓  |
| Very easy deployment                                       | ✓          | ✓                       | ✓  |
| Can be used with old SPs (<2.4)                            | ✓          | (✓)                     |  |
| Categories supported                                       | (✓)        | ✓                       |  |
| Uses cached recent IdP selection across different services |            | ✓                       |  |

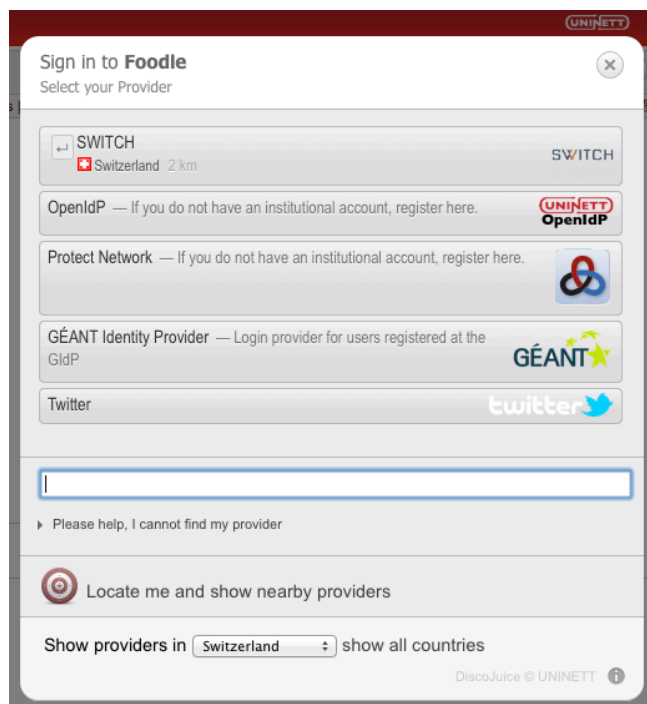
## When to use what ?

| Numbers of IdPs | Login Link(s) | Embedded WAYF<br>SWITCH | EDS<br> Shibboleth. |
|-----------------|---------------|-------------------------|--|
| 1 - 5           | ✓             | ✓                       | ✓  |
| 1 - 500         |               | ✓                       | ✓  |

## To mention: Disco Juice

- Very comprehensive Discovery Service
- Well suited for services with users from many IdPs
- Search-as-you-type only
- Uses Geo IP and metric to guess user's IdP
- Based on PHP and JS

 <http://discojuice.org/>



# Interfederation Attributes

And how to use the Shibboleth Attribute Checker



# SWITCH

SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)

# Recommended Interfederation Attributes

EduGAIN recommends these attributes for each user:

| Friendly name   | Defined in | Example   |
|---|------------|---|
| <b>displayName</b>  | eduPerson  | Beatrice Huber  |
| <b>common name (cn)</b>                                   | eduPerson  | Beatrice Huber  |
| mail  | eduPerson  | bea.huber@switch.ch   |
| eduPersonAffiliation<br><b>eduPersonScopedAffiliation</b> | eduPerson  | staff<br>staff@switch.ch  |
| <b>eduPersonPrincipalName</b>                             | eduPerson  | 234cd8z239@switch.ch  |
| <b>schacHomeOrganization</b>                              | SCHAC      | switch.ch   |
| <b>schacHomeOrganizationType</b>                          | SCHAC      | urn:mace:terena.org:schac:home<br>OrganizationType:int:NREN   |
| eduPersonTargetedID /<br>Persistent Name ID               | eduPerson  | https://aai-logon.switch.ch/idp/<br>shibboleth!https://sp.example.org/<br>shibboleth!2389cdhu3e-sda7323 |

## eduGAIN-specific Attributes

- Difference **commonName/displayName**:  
The same but commonName might be multi-valued
- **eduPersonScopedAffiliation**:  
Like eduPersonAffiliation but with domain name appended
- **eduPersonPrincipalName**:  
Like eduPersonAffiliation but with domain name appended
- **schacHomeOrganization**:  
Domain name (like swissEduPersonHomeOrganisation)
- **schacHomeOrganizationType**:  
Not very well defined yet unfortunately...

## Make SP eduGAIN attributes

- The attributes in bold blue letters are normally not used in SWITCHaai
- To make SP support them, the attribute-map.xml must be adapted to contain their definition
- SWITCHaai configuration guide can do that for you:  
Choose "Interfederation/eduGAIN Support" during configuration to include definitions automatically

### Advanced Configuration Options

Enable SWITCHtoolbox Tool Support:

☐ Configure Service Provider as SWITCHtoolbox Tool. [More ...](#)

Enable Interfederation/eduGAIN Support:

☒ Configure Service Provider for Interfederation. [More ...](#)

[Update Configuration Guide with above Data](#)

## Missing Attributes on SP

- Attribute release in other federations unfortunately is often a manual process
  - Identity Providers in other federations often don't release attributes
  - Not so much an issue in SWITCHaai thanks to Resource Registry
- Consequence: SPs sometimes don't get required attributes
  - Users will get some error from application or SP
- Ideally, application shows an error that tells what attributes are missing
- But Shibboleth SP can do that too

# Check Available Attributes

- In `<ApplicationDefaults>` or `<ApplicationOverride>` add the configuration option:  
`sessionHook="#URL#"`
- User is redirected to this (absolute or relative) URL
  - Before he is redirected to page requested initially
  - Page should check if all attributes are available and show error if not
  - Page therefore needs access to user's attributes!
- Standard page provided by Shibboleth would be:  
`sessionHook="/Shibboleth.sso/AttrChecker"`
  - Can use boolean expressions to check attributes

# Attribute Checker Example

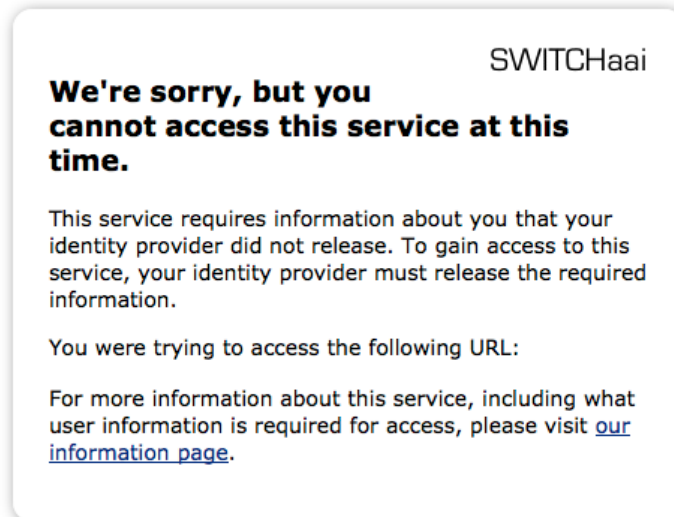
If condition is not met:

- Shows an error message
- Flushes the Shibboleth session

```
<Handler type="AttributeChecker" flushSession="true"
  Location="/AttrChecker" template="attrChecker.html">
  <OR>
    <Rule require="displayName"/>
    <AND>
      <Rule require="givenName"/>
      <Rule require="surname"/>
    </AND>
  </OR>
</Handler>
```

# Standard Error Message

- Template is: `/etc/shibboleth/attrChecker.html`
- Ideally mention which attributes are missing



## SWITCHtoolbox and Group Management Tool

Light weight group management, access control and authorization



# SWITCH

SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)

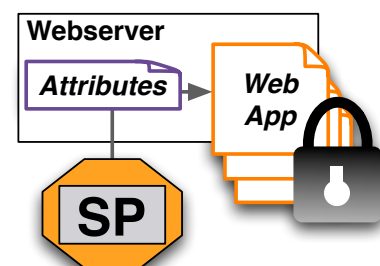
# Agenda

- The problem statement
- Two major cases
  - common attribute value(s) exists
  - no common attribute value(s) exists
- Two solutions
  - Introduce a common attribute value
  - Still no common attribute
    - \* Manage the group 'by hand'
    - \* Manage it with 'Group Management Tool' or 'Toolbox'

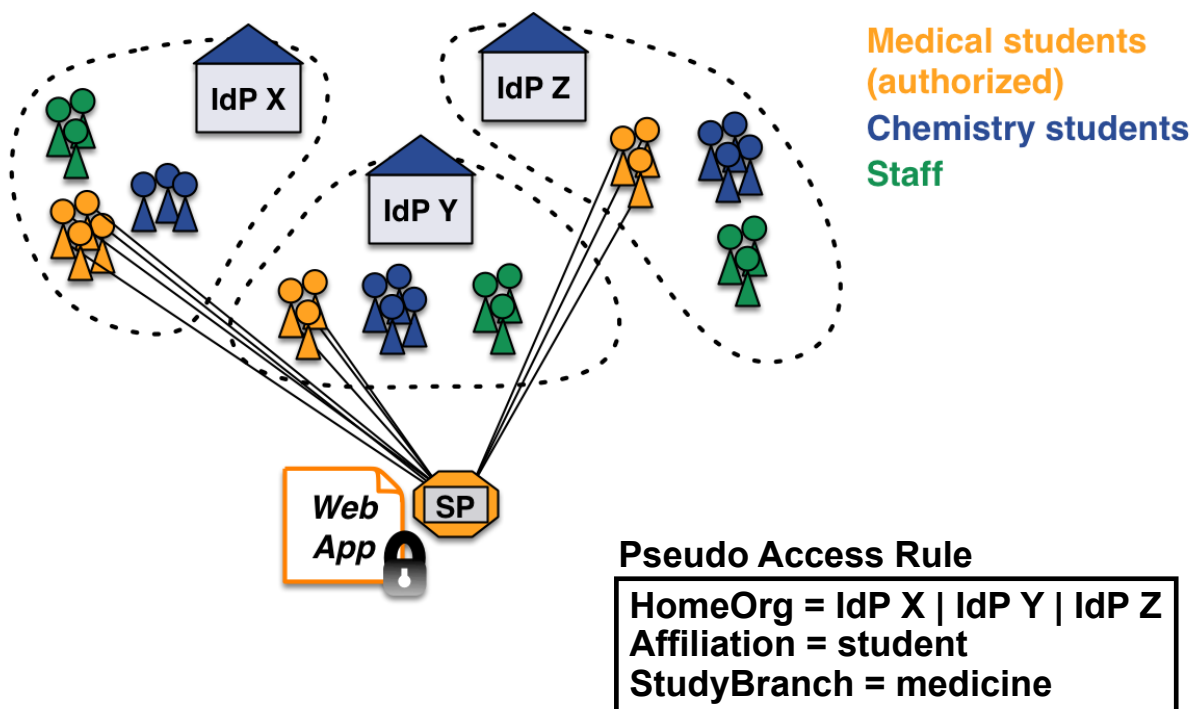
## Situation

- Grant access to a specific group of people
- All users have an AAI account
- Overhead for group administration should be small

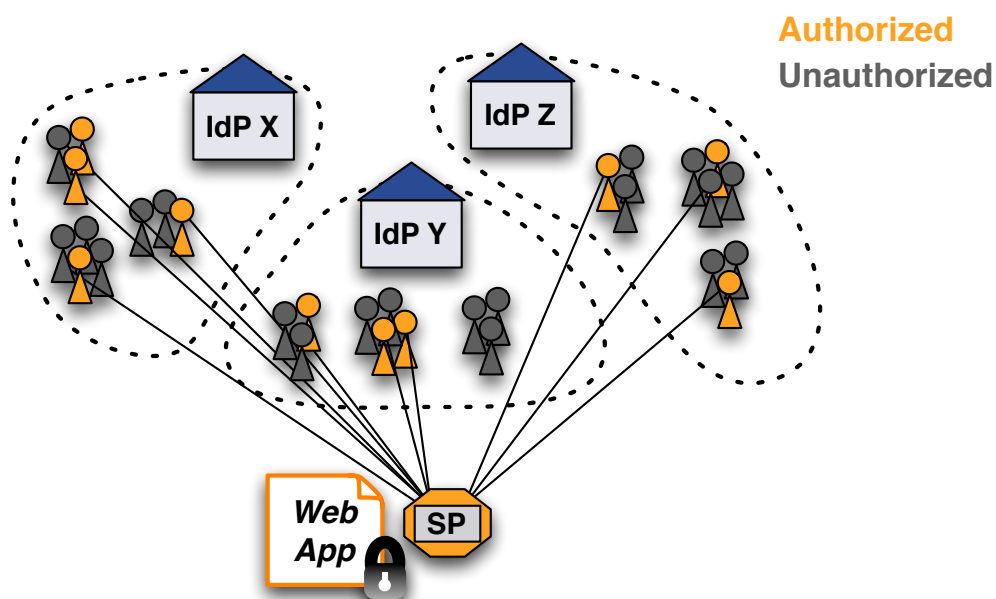
- **Real life example:**
  - *The slides of this workshop shall only be accessible by all people who attended the workshop.*



## Case 1: Users share common attributes



## Case 2: No common user attributes



Without a shared user attribute, no simple access control rule can be created



## Solution 1: Create a common attribute

- Add a common attribute to user's identity, e.g. an entitlement attribute

### Pseudo Access Rule

**Require entitlement *urn:mace:rediris.es:entitlement:wiki:jra5***



- Very simple solution



- Additional work for user directory administrator
- Difficult to efficiently manage many entitlement values
- Only IdP admin can manage access
- **Only works for users from same organisation**

## Solution 2.a: Use uniqueIDs or email

1. Get unique IDs or email addresses from users
2. Create access rules like:

**Note:** Email address is less suited, it might get reassigned!

### Pseudo Access Rule

**require uniqueID *465@idpx.ch 234@idpy.ch [...]***  
**require email *hans.muster@idpx.ch pierre.m@idpz.ch [...]***



- Straight-forward solution

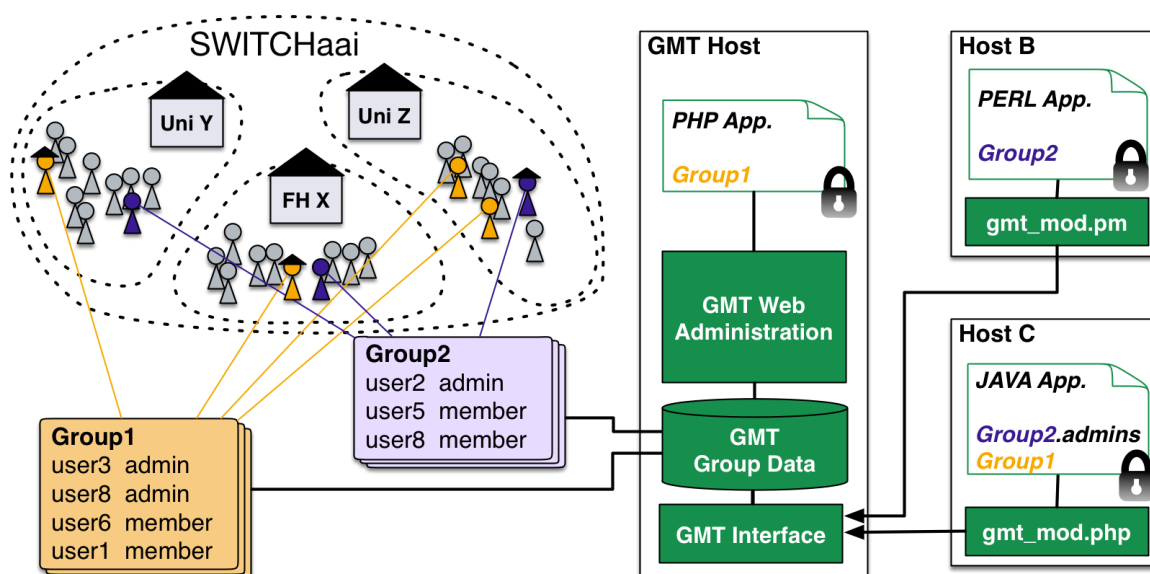


- SP administrator must know unique ID/email address
- Difficult to efficiently manage for many users/apps
- **Only the SP admin can manage access**

## Solution 2.b: Group Management Tool

- Web based open source PHP tool developed by SWITCH
- Manages multiple groups to protect multiple applications
- Users can be:
  - invited to a group via email
  - added to a group with a shared group password
  - added to a group based on their attributes
  - moderated after they request to join a group
- GMT generates authorization files (for Apache and Shibboleth SP)
  - this option only works on the same host as the GMT
- API and libraries for authorization on remote hosts

## GMT Overview



<https://www.switch.ch/aai/gmt>

# GMT Administration Interface

## SWITCH Group Management Tool

Administration Interface

Overview

Add new group

Invite users

Add users

Show roles

Export all groups

Need help?

| Group                     | Members | Authorization Files | Actions                |
|---------------------------|---------|---------------------|------------------------|
| ExportGroup               | 3       | Add                 | Manage Settings Remove |
| OLAT                      | 2       | Add                 | Manage Settings Remove |
| Test Group 1              | 2       | Manage 1 files      | Manage Settings Remove |
| Test Group 2              | 3       | Add                 | Manage Settings Remove |
| Test Group 3              | 2       | Manage 1 files      | Manage Settings Remove |
| Registered Users          | 6       | Add                 | Manage Settings        |
| Pending User Requests     | 3       | -                   | Manage -               |
| Pending Invitation Tokens | 5       | -                   | Manage -               |

© 2008 SWITCH GMT V1.1

Logged in as: **Lukas Hämmerle** (Global Administrator role class)

## GMT Authorization File Example

- Multiple groups can write to same authorization file
- Example of an .htaccess file

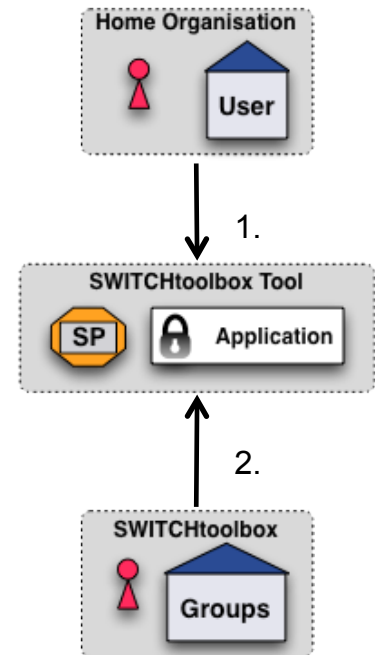
```
# Group Management Tool: Apache Authorization File
# DON'T EDIT LINES THAT CONTAIN ###
# AND ALSO DON'T REMOVE THE FOLLOWING TWO DIRECTIVES
AuthType shibboleth
ShibRequireSession On

require placeholder never.match

###START:Test_Group_1###
require uniqueID 023sdf-345fdg-23401@unizh.ch
require uniqueID 3141324sdd592@ethz.ch
###END:Test_Group_1###
```

## Solution 2.c: SWITCHtoolbox

- Service Provider aggregates:
  - identity information from users's IdP
  - group information from SWITCHtoolbox IdP
- Application receives group membership information like any other Shibboleth attribute
- Everybody can create groups
- Allows easy access control rules



### Pseudo Access Rule

**require isMemberOf https://toolbox.switch.ch/mygroup**

## SWITCHtoolbox Administration

Home | News | Contact | All Services by SWITCH | de | fr | it | en

SWITCH

SWITCHtoolbox

Early Adopters | Lukas Hämmerle | Logout | Help

↑ About SWITCHtoolbox

Home > Early Adopters

Home | Early Adopters


**Early Adopters** [Edit]

This open group is for people who want to testdrive SWITCHtoolbox.

Contact Rolf Brugger  
Contact Mail rolf.brugger@switch.ch

[Additional Information](#)

**Profile** [Edit]

 **Lukas Hämmerle**  
Administrator  
lukas.haemmerle@switch.ch  
Enrolled

**Activities**

3 days ago  
Yves Ettounsi joined group 'Early Adopters'

about 1 month ago  
Rolf Brugger removed Rolf Brugger from the subgroup 'Administrators' of the group 'earlyadopters'

about 1 month ago  
Rolf Brugger removed Rolf Brugger from group 'Early Adopters'

4 months ago  
Lukas Hämmerle removed Hämmerle from group 'Early Adopters'

4 months ago  
Lukas Hämmerle invited Hämmerle into group 'Early Adopters'

## Add a Service as Tool

- SP needs only minor config changes to become a tool
- Tool can be public or private
  - Public tools can be subscribed/accessed by many different groups
- SWITCH offers these public tools:
  - Document Filing, Discussion Forum, Mailinglist, SWITCHinteract, SWITCHcast, Wiki

<https://www.switch.ch/toolbox/>

## Summary

- GMT and SWITCHtoolbox are similar
- GMT has to be installed and maintained yourself
  - Allows customization
  - Suited for few groups with few users
  - Only protects applications on same host or requires libraries
- SWITCHtoolbox is a service offered by SWITCH
  - Allows easier integration of application
  - Can manage many of groups and sub groups of moderate size
  - No software libraries required to protect remote applications
  - Multilingual

<https://www.switch.ch/aai/guides/sp/access-rules/>

# SP Logout Support

## Possibilities and Limitations



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Single Logout: Is it possible?

### **Single Logout will work reliably in some cases only!**

Currently, Single Logout is not well supported in SWITCHaai, because...

- The Shibboleth Identity Provider software doesn't yet provide full-featured support.
  - This might change in the near future with IdPv3.
- Most Identity Providers in SWITCHaai don't yet support Single Logout

# Single Logout: Is it possible?

## Limited logout may be better than no logout at all!

You may want to support Single Logout for critical applications of your own organization.

- The organization's Identity Providers needs some configuration changes.
- The Identity Provider needs to publish the service locations for Single Logout.

## Agenda

- Single Logout in Federation
- Single Logout Issues
- Single Logout for SP
- Support Resources

## Single Logout in Federation

- Users access multiple services, but need to login once only
- They might be logged in to multiple services
- ... but how do they logout again from all services?
- The solution seems to be easy:
  - The user initiates the single logout process
  - The user is logged out from all services and the IdP in turn
- But:
  - Where does the user start the single logout process?
  - Who knows all of the services the user is currently logged in?
  - Should the user be logged out from all services in the federation, or also from Google Mail, Facebook, etc.?
  - What happens if an error occurs during the whole logout process?
- Logout will be possible but it has a lot of limitations!

## SAML 2 SLO Messages and Flow

- SAML 2 SLO may be initiated by either the Identity Provider (IdP) or the Service Provider (SP)
- SP-initiated SLO:
  - An SP sends a logout request to the IdP
  - At the IdP, for each SP to which the user has authenticated:
    - The IdP sends a logout request to the SP
    - The SP attempts to destroy its session for the user and sends back a logout response indicating if this was successful
  - The IdP destroys its session for the user
  - The IdP sends a logout response to the initiating service provider, which then destroys its session
- It is the responsibility of the SLO initiator to provide the user with information about whether SLO has succeeded or failed.



## SLO Issues: User Experience

### What does a user expect when clicking on logout?



- Logout only from this single application?
  - Is of little use because of Single Sign On
- Logout from all applications where logged in? Which?
  - Also from Google Mail, eBay and other non AAI applications?

### Therefore:

- Users must understand the consequences of logout
  - Must know that they currently are signed in to a single sign-on (SSO) system and what will result from clicking on logout
- Users must always know if logout has completely succeeded
  - Otherwise they may assume that it has and leave the computer, allowing someone else to erroneously access a service

## SLO Issues: Logged in vs. Logged out

### What defines if a user is logged in via AAI/application?

-  Shibboleth session cookie
-  Application session cookie (optional)
  - Some applications only check if user was authenticated via AAI

### What is necessary to log out a user?

- Delete Shibboleth and application cookies (front-channel)
  - Only possible when user's browser is involved
    - Administrative logout not possible
- Or delete session information on server (back-channel)
  - Only possible if user's Shibboleth sessionID is known in application
    - Implies adaptation of application

## SLO Issues: Technical Difficulties

### Front-Channel vs. Back-Channel problems

- Front-Channel: Protocol flow via browser
  - Process might break
  - User might get confused
- Back-Channel: Direct communication between SP and IdP
  - User's session cookie is not available

### SP session vs. application session

- The SP and the web application often manage separate sessions
- SLO must make sure that both sessions are destroyed

## The two flavors of logout

### Local logout

- User's session is deleted only for one Service Provider
  - Not of much use due to Single Sign-On (SSO)
  - Or "egoistic" if IdP session also is bilaterally deleted but all other SP's session are still intact.

### Global logout = Single Log Out (SLO)

- User's SSO session deleted on IdP and **all** SPs
  - For authentication methods like HTTP Basic Auth or some external authentication systems, the IdP cannot destroy the SSO session!
    - Only safe way for logout is to cleanly exit the web browser or even to logout from the system!

## Current state of SLO in Shibboleth

### **Shibboleth Service Provider 2.5.x**

- Supports local and global logout

### **Shibboleth Identity Provider 2.4.x**

- Supports local and global logout
- Doesn't support "full" SAML 2 logout, i.e. doesn't support logout from multiple Service Providers

### **Shibboleth Identity Provider 3.x**

- Currently, same limited support as 2.4.x.
- Full support should get available in the near future.

## Current state of SLO in applications

### **Adapted Applications:**

- Some well-known applications (less than 10) are ready to support SAML 2 logout (incl. Moodle, ILIAS, Resource Registry)
- Custom applications need to be adapted.

## Enabling Single Logout on the SP

### Enable SLO for SP to support global logout:

- Add "SAML2" to the existing <Logout> element in the Shibboleth SP configuration in /etc/shibboleth/shibboleth2.xml

```
<Logout>SAML2 Local</Logout>
```

- SAML 2 logout is initiated by accessing the following URL:  
<https://ilias.example.com/Shibboleth.sso/Logout>
  - If the IdP supports SAML 2 logout, too, then SAML 2 logout starts.
  - Else, local logout is done (and local logout page is shown).
- By default, the IdP doesn't return to the SP
  - SP can be configured to force returning (IdP possibly returns with "partial logout" status)


## Enabling Single Logout in the web application

### If the application manages its own session, it needs to be adapted or configured to support single logout

- The application needs to implement a "logout notification handler"  
<https://wiki.shibboleth.net/confluence/display/SHIB2/SLOWWebappAdaptation>
  - SP notifies the application about logout through a "back-channel"
  - Application needs to destroy the session
- Some applications, like Moodle and ILIAS, have built-in support (see documentation)
- Notification must be enabled in the Shibboleth SP configuration in /etc/shibboleth/shibboleth2.xml

```
<Notify  
  Channel="back"  
  Location="https://ilias.example.org/.../shib_logout.php"/>
```

## Example Landing Page on IdP

Example

SWITCHaai

**Abmeldung**

Sie haben sich vom Anmelde-Dienst (Identity Provider) abgemeldet. Möglicherweise sind Sie aber noch bei einem oder mehreren der folgenden Dienste angemeldet:

- **AAI Attributes Viewer** (<https://aai-viewer.switch.ch/shibboleth>)
- **Resource Registry** (<https://rr.aai.switch.ch/shibboleth>)

Bitte beachten Sie folgendes:

**Falls Sie an einem Computer arbeiten, der von mehreren Personen verwendet wird (z. B. Computer in Internet Café):**  
Bitte melden Sie sich ganz ab (Abmeldung von Mac OS X) und starten Sie evtl. den Computer neu. Ansonsten ist es möglich, dass fremde Personen später auf Ihre persönlichen Daten zugreifen können, da Sie möglicherweise trotzdem noch bei anderen Diensten angemeldet sind.

**Falls Sie an Ihrem privaten Computer arbeiten, der nur von Ihnen verwendet wird:**  
Wenn Sie sicher sein möchten, dass Sie auch von anderen Diensten abgemeldet sind, empfehlen wir Ihnen, die Chronik des Browsers (insbesondere Cookies) zu löschen, oder den Computer neu zu starten. (Es reicht teilweise nicht aus, nur den Browser zu schliessen.)

## Conclusion

- Single Logout is partially possible
- Works well if user is logged in to one application only
- It's still better to get logged out from the IdP than not to log out at all

## Support Resources

- Single Logout Issues
  - <https://wiki.shibboleth.net/confluence/display/SHIB2/SLOIssues>
- Single Logout for Shibboleth SP
  - Configuration of SP Logout Initiator  
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPLogoutInitiator>
  - Adaptation of Web Application  
<https://wiki.shibboleth.net/confluence/display/SHIB2/SLOWWebappAdaptation>
  - Logout notification to application  
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPNotify>
- Single Logout for Shibboleth IdP
  - <https://wiki.shibboleth.net/confluence/display/SHIB2/IdPEnableSLO>

## SP Virtualization

Running multiple SPs on a single host



# SWITCH

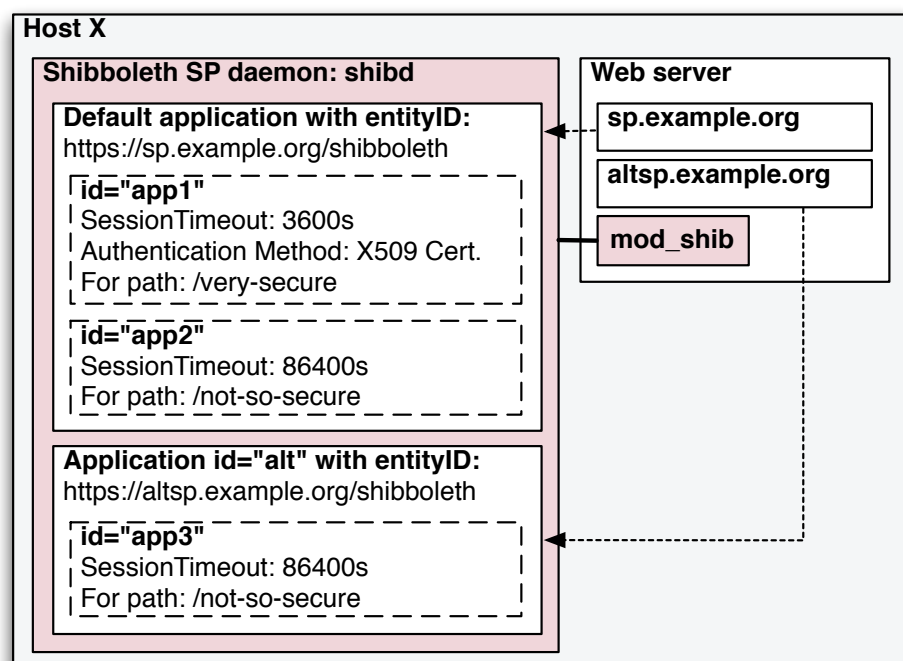
SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)

# Physical vs. logical SP

A single physical SP can host any number of logical SPs

- A logical SP can then include any number of “applications”
- Applications can be configured on a per-path or per-virtual-host basis
- Web virtual hosting is often related but is also independent
- Applications can inherit or override default configuration settings on a piecemeal basis

## Multiple applications and domains on a single host



# shibboleth2.xml configuration

Add an **ApplicationOverride** element for each logical SP, and specify its own **CredentialResolver**:

```
<ApplicationDefaults id="default" policyId="default" ... >
  ...
  <ApplicationOverride id="altsp"
    entityID="https://altsp#.example.org/shibboleth">
    <CredentialResolver type="File"
      key="/etc/shibboleth/altsp-key.pem"
      certificate="/etc/shibboleth/altsp-cert.pem"/>
    </ApplicationOverride>
  </ApplicationDefaults>
```

Note: when adding a customized **Sessions** element to the **ApplicationOverride**, be sure to spell out *all* its attributes. Inheritance from **ApplicationDefaults** is disabled as soon as a **Sessions** element is present.

# Apache httpd configuration

Define an additional **VirtualHost** for the logical SP, and map it to the respective **ApplicationOverride** from shibboleth2.xml:

```
<VirtualHost *:443>
  ServerName altsp#.example.org:443
  ...

  <Location />
    ShibRequestSetting applicationId altsp
  </Location>

</VirtualHost>
```



# IIS Site Mapping

In shibboleth2.xml, add a **<Host>** element for the logical SP (with the **name** attribute matching the IIS site name):

```
<RequestMapper type="Native"
  <RequestMap>
    <Host name="sp#.example.org">
      <Path name="secure" authType="shibboleth"
        requireSession="true"/>
    </Host>
    <Host name="altsp#.example.org" applicationId="altsp">
      <Path name="secure" authType="shibboleth"
        requireSession="true"/>
    </Host>
  </RequestMap>
</RequestMapper>
```



6

## Recommendations

- use separate Apache **VirtualHosts** / IIS sites to run multiple, but distinct AAI-protected resources on a single host (avoid path-based separation of applications)
- define separate entity IDs for each resource, and create key pairs (self-signed certificates) for each of them
- register and manage each resource / logical SP in the AAI RR as a separate entity with its respective attribute requirements
- Further reading:  
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplicationOverride>



7

# SP Error Handling

Error page templates and customization



# SWITCH

SWITCHaai Team

[aai@switch.ch](mailto:aai@switch.ch)

 © SWITCH 2015

## shibd Error Handling

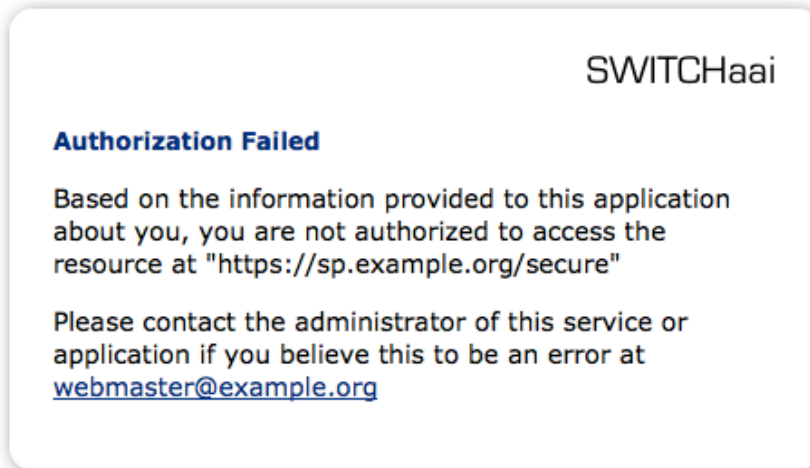
- fact of life: things can go wrong when running a Shibboleth SP
- `shibd/mod_shib` includes error handling for four types of errors:
  - authorization failures: `accessError.html` (“Authorization Failed”)
  - metadata-related errors: `metadataError.html` (“Unknown or Unusable Identity Provider”)
  - non-redirectable non-SSL requests: `sslError.html` (“POST Failed”)
  - general processing errors: `sessionError.html` (text depends on specific error)

 © SWITCH 2015

2

# Standard `accessError.html`

- default error description is fairly vague



## Customizing the error page(s)

- content of the HTML templates in `/etc/shibboleth` can be adapted by taking advantage of `<shibmlp tagname />` elements
- list of available `tagnames` (about a dozen):  
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPErrors>
- some of them might sometimes be undefined (contactName and contactEmail of the IdP e.g.), so use `<shibmlpif tagname>...</shibmlpif>` if needed

## Other error handling options

- as an alternative to using the templates, set the `redirectErrors="..."` attribute on the `<Errors>` element in `shibboleth2.xml` to define a handler URL which is passed the error details as GET parameters:  
`https://example.org/error?now=...&requestURL=...&errorType=...&...`
- extend your application logic to deal with the case of an attribute missing from the environment – and display your own specific error message, possibly giving more details as to what attributes are missing, or why certain attributes do not have the required values (affiliation "staff" e.g.)

## Conclusion

- error template customization: adapting `accessError.html` is useful for cases where attribute requirements are uniformly applied to all protected content
- for more sophisticated diagnostics (for the user), extending the application's error handling allows more fine-grained control

# Shibboleth-aware Applications

Some Examples



# SWITCH

SWITCHaai Team

lukas.haemmerle@switch.ch

## Applications already Shibboleth-ready

- Official list:  
<https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled>
  - List is not up-to-date and not complete
  - Contains (hosted) services as well as OSS/commercial software
  - Applications that make use of HTTP Basic Auth (e.g. Nagios) are not listed but they are very easy to "shibbolize" using the REMOTE\_USER attribute
  - If your application is not on the list google for application name and "Shibboleth" or "SAML"
- What does Shibboleth-enabled mean exactly?
  - Especially commercial products often "exaggerate" to sell more
  - Many products rely on Shibboleth, other's implement a small fraction of the SAML standard. Often they work only with individual IdPs
  - Often, SAML is used only for authentication but not for authorisation

# Shibboleth-enabled out-of-the-box?

- **Most Shibboleth/SAML-enabled application use:**
  - Shibboleth Service Provider: Recommended for SWITCHaai
  - SimpleSAML PHP: Popular PHP-only alternative implementation

**Careful:** Most commercial web-hosters don't support Shibboleth SP because Shibboleth Apache/shibd process need to be installed.
- **Some applications support SAML natively**
  - OCLC EZproxy: Popular proxy for accessing e-journals
  - Microsoft ADFS: Required for Sharepoint
- Non-Shibboleth SAML implementations often are not fully interoperable or have a limited feature set

## Example: Moodle

- Popular e-Learning application in SWITCHaai (>40SPs)
- Requires installation of a Shibboleth Service Provider
  - Use our installation and configuration guide
  - Then follow the instructions in the README of the Moodle Shibboleth plug-in to protect `/auth/shibboleth/index.php`
- Configuration is done via web interface:
  - Site Administration – Plugins – Authentication – Shibboleth
- SWITCH heavily contributed to initial version of plugin

# Moodle Configuration

- Configuration is done via web interface:  
Site Administration – Plugins – Authentication – Shibboleth
- This plug-in only covers authentication!
  - Other plugins to enrol user based on Shibboleth attributes
- Configuration defines:
  - Discovery Service: Use internal or external one
  - Alternative Login/Logout URLs: To further customize behavior
  - Attribute mapping: Shibboleth Attribute -> User profile field
  - Attribute update/locking: If and when to update user profile field
  - Data modification hook: To transform attributes before use in Moodle

## Moodle Screenshot: Configuration I

|  |   |
|--|---|
| Username: <input type="text" value="Shib-SwissEP-UniqueID"/>   | Name of the webservice Shibboleth environment variable that shall be used as Moodle username  |
| Data modification API: <input type="text" value="/opt/www/convert_data2.php"/>   | You can use this API to further modify the data provided by Shibboleth. Read the <a href="#">README</a> for further instructions.off  |
| Moodle WAYF service: <input type="checkbox"/>  | If you check this, Moodle will use its own WAYF service instead of the one configured for Shibboleth. Moodle will display a drop-down list on this alternative login page where the user has to select his Identity Provider.   |
| Identity providers: <input type="text" value="https://aai-demo-idp.switch.ch/idp/shibboleth, AAI Demo Home Organisation, /Shibboleth.sso/DS https://aai-test-idp.switch.ch/idp/shibboleth, AAI Test Home Organisation, /Shibboleth.sso/DS https://aai-logon.vho-switchaai.ch/idp/shibboleth, Virtual Home Organisation @SWITCHaai, /Shibboleth.sso/DS"/> | Provide a list of Identity Provider entityIDs to let the user choose from on the login page. On each line there must be a comma-separated tuple for entityID of the IdP (see the Shibboleth metadata file) and Name of IdP as it shall be displayed in the drop-down list. As an optional third parameter you can add the location of a Shibboleth session initiator that shall be used in case your Moodle installation is part of a multi federation setup. |
| Shibboleth Service Provider logout handler URL: <input type="text" value="https://ebulobo.switch.ch/Shibboleth/Logout"/>   | Provide the URL to the Shibboleth Service Provider logout handler. This typically is /Shibboleth.sso/Logout   |
| Alternative logout URL: <input type="text"/>   | Provide the URL that Shibboleth users shall be redirected to after logging out. If left empty, users will be redirected to the location that moodle will redirect users to  |
| Authentication method name: <input type="text" value="AAI Login"/>   | Provide a name for the Shibboleth authentication method that is familiar to your users. This could be name of your Shibboleth federation, e.g. SWITCHaai Login or InCommon Login or similar.  |
| Password-change URL: <input type="text"/>  | Here you can specify a location at which your users can recover or change their username/password they've forgotten it. This will be provided to users as a button on the login page and their user page. If you leave this blank the button will not be printed.   |

# Moodle Screenshot: Configuration I

**Data mapping**

|               |  |
|---------------|--|
| First name    | <input type="text" value="givenName"/>           |
| Update local  | <input type="button" value="On every login"/>    |
| Lock value    | <input type="button" value="Unlocked if empty"/> |
| Surname       | <input type="text" value="surname"/>             |
| Update local  | <input type="button" value="On every login"/>    |
| Lock value    | <input type="button" value="Unlocked if empty"/> |
| Email address | <input type="text" value="mail"/>                |
| Update local  | <input type="button" value="On creation"/>       |
| Lock value    | <input type="button" value="Unlocked if empty"/> |
| City/town     | <input type="text" value=""/>                    |
| Update local  | <input type="button" value="Unlocked"/>          |
| Lock value    | <input type="button" value="Unlocked if empty"/> |

# ILIAS Screenshot: Role Assignment

**Edit Role Assignment Rule**

|                      |  |
|----------------------|--|
| ILIAS Role Name *    | <input checked="" type="radio"/> Global Role<br><input type="text" value="Administrator"/>   |
|                      | <input type="radio"/> Local Role<br>Please choose either a global role or enter the name of a local role.  |
| Role Assignments     | Assignment of Roles After Later Logins<br><input checked="" type="checkbox"/> Assign Missing Roles<br><input type="checkbox"/> Deassign Deprecated Roles                             |
| Kind of Assignment * | <input checked="" type="radio"/> User Attribute<br>Assign by a specific attribute in the Shibboleth User Profile.<br>Attribute Name <input type="text" value="Shib-EP-Entitlement"/> |



# IdP Version 3 Upgrade

## General observations



# SWITCH

SWITCHaai Team  
aai@switch.ch

## IdP V3, a new milestone

- IdP version 2.0.0 released in March 2008
  - followed by 4 minor releases and 18 patch releases (current is 2.4.4)
- IdP version 3: the first major release after ~7 years
  - 3.0.0: December 2014, only very sparse documentation in the Wiki
  - 3.1.0/3.1.1: March 2015, now being deployed for production use, documentation considerably improved in Q1/Q2 2015
- a good opportunity to start with a fresh environment
  - requires Java 7 or later and Servlet API 3.0 support
  - best run on a platform with an expected lifetime of 5+ years
- *do not* consider an in-place upgrade of your IdP v2 deployment
  - even if the Shibboleth installer claims supporting this to some extent

# Operating system recommendations

- rely on an OS with long-term support (5+ years)
- use the same Linux distribution / one from the same family which your organization is already using for other services
- the SWITCH deployment guide has been rewritten to cover
  - Ubuntu Server 14.04 LTS  
released in April 2014, supported through April 2019
  - Red Hat Enterprise Linux 7 / CentOS 7  
released in June 2014, supported through June 2024
- Debian is no longer covered in the SWITCH guide
  - very similar to Ubuntu, though (in case you have strong feelings about staying with Debian)

# Java and Webapp environment

- rely on the operating system's default Java version
  - for both Ubuntu 14.04 and RHEL 7, this is OpenJDK 7
  - Java 8 has potential pitfalls with scripted attributes (Rhino/Nashorn engine incompatibilities), so better stay with Java 7 for the time being
- use a Java Servlet container which is provided in the form of a package supported by the OS vendor
  - Tomcat 7 is the primary container for both supported OSes
  - you don't have to bother about manually applying security patches for the Servlet container
- run Apache httpd in front of the Servlet container
  - flexible configuration of the TLS endpoints for the IdP
  - mod\_proxy\_ajp has proven robust with the IdP v2 in the past

# Persistent ID and user consent storage

- the IdP requires a relational database for storing persistent identifiers and user consent data
- for a single-instance IdP, install an SQL database which is packaged by the OS vendor
- starting with the IdP v3 deployment guide, and when installed on the same system as the IdP, SWITCH is favoring PostgreSQL
  - PostgreSQL has a long track record of close SQL standards compliance
  - MariaDB 5.5 (community-developed source fork of MySQL) would also be available as a vendor-supplied package, but for Ubuntu, only in the “universe” component – i.e., without official support for security updates
- your favorite RDBMS can be used as well, of course
  - a JDBC connector is almost all it takes
  - in particular for clusters, other RDBMSes might be better fits

# Testing strategy

- `/etc/hosts` is your friend
- Set up the IdP v3 on a completely new system
- retain the existing entity ID, SAML endpoints and the SAML certificate
- with SAML 2, most IdP traffic is now front channel
  - straightforward testing possible by simple edits of your `hosts` file:  
`192.0.2.3 aai-login.example.org`
- for back-channel testing, a temporary change to an SP's `hosts` file can be an option

# IdP Configuration Pattern

Get used to Spring, Beans and Properties



# SWITCH

SWITCHaai Team  
aai@switch.ch

```
<!-- Connection Configuration -->
<bean id="connectionConfig"
      class="org.ldaptive.ConnectionConfig"
      abstract="true"
      p:ldapUrl="%{idp.authn.LDAP.ldapURL}"
      p:useStartTLS="%{idp.authn.LDAP.useStartTLS:true}"
      p:useSSL="%{idp.authn.LDAP.useSSL:false}"
      p:connectTimeout="%{idp.authn.LDAP.connectTimeout:3000}"
      p:sslConfig-ref="sslConfig" />

<!-- Attribute Resolver Configuration -->
<util:list id="shibboleth.AttributeResolverResources">
  <value>%{idp.home}/conf/attribute-resolver-switchaai-core.xml</value>
  <value>%{idp.home}/conf/attribute-resolver-connectors.xml</value>
  <value>%{idp.home}/conf/attribute-resolver-other.xml</value>
</util:list>

<!-- Attribute Filter Configuration -->
<util:list id="shibboleth.AttributeFilterResources">
  <ref bean="FileBackedSWITCHaaiAttributeFilter"/>
</util:list>
```

## What's that?

## Configuration Pattern of IdPv3

- The IdPv3 configuration builds upon the "Spring Framework"
  - Configuration is located in XML files
  - There are a lot of wired "beans"
- The whole configuration follows the same pattern
  - With some few exceptions
- Wonderfully flexible way to configure components  
... **but: quite complicated for deployers!**

## Understanding Beans and Properties

### **Bean:**

Some software object that is configurable by setting its attributes.

### **Property:**

A piece of information, keyed by some name  
(e.g. `idp.authn.LDAP.useSSL = true`)

# Understanding Beans and Properties

- The whole configuration of the IdP is specified by a lot of beans.
- For convenience, the essential configuration can be specified by properties stored in properties files.
- Still, from time to time, you will need to directly modify beans or create new ones.
- The beans are specified in XML notation, and the corresponding software objects are created at runtime when the IdP starts.

## Examples of Properties

Configuration file

`/opt/shibboleth-idp/conf/ldap.properties:`

```
# LDAP connection parameters
idp.authn.LDAP.ldapURL      = ldaps://ldap-test2.aai.switch.ch:636
idp.authn.LDAP.useStartTLS  = false
idp.authn.LDAP.useSSL       = true
idp.authn.LDAP.sslConfig    = jvmTrust
idp.authn.LDAP.baseDN       = ou=People,dc=example,dc=org
idp.authn.LDAP.subtreeSearch = true
idp.authn.LDAP.userFilter   = (uid={user})
idp.authn.LDAP.bindDN       = cn=idp,dc=example,dc=org
```

- Each line consists of a pair of a key and a value.
- Comment lines start with an # character.

# Examples of Beans

## Configuration file

`/opt/shibboleth-idp/conf/authn/ldap-authn-config.xml:`

```
<!-- Connection Configuration -->
<bean id="connectionConfig"
      class="org.ldaptive.ConnectionConfig"
      abstract="true"
      p:ldapUrl="%{idp.authn.LDAP.ldapURL}"
      p:useStartTLS="%{idp.authn.LDAP.useStartTLS:true}"
      p:useSSL="%{idp.authn.LDAP.useSSL:false}"
      p:connectTimeout="%{idp.authn.LDAP.connectTimeout:3000}"
      p:sslConfig-ref="sslConfig" />
```

- Each bean has some name ("id")
- Each bean has some type ("class")
- Attributes (parameters) specify the bean's configuration
- Beans can refer to other beans (wiring)

# Examples of Beans

- There are some helper constructs to define beans.

Example:

Beans that are lists of values or lists of other beans.

## Configuration file

`/opt/shibboleth-idp/conf/services.xml:`

```
<util:list id="shibboleth.AttributeResolverResources">
  <value>%{idp.home}/conf/attribute-resolver-switchaai-core.xml</value>
  <value>%{idp.home}/conf/attribute-resolver-connectors.xml</value>
  <value>%{idp.home}/conf/attribute-resolver-other.xml</value>
</util:list>

<util:list id="shibboleth.AttributeFilterResources">
  <ref bean="FileBackedSWITCHaaiAttributeFilter"/>
</util:list>
```

## References

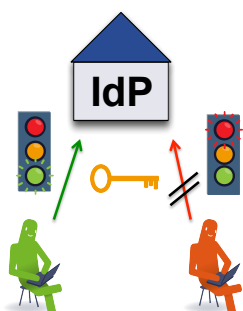
For comprehensive information, refer to the documentation on the Shibboleth Wiki.

### Documentation

- **Configuration**  
<https://wiki.shibboleth.net/confluence/display/IDP30/Configuration>
- **Spring Configuration**  
<https://wiki.shibboleth.net/confluence/display/IDP30/SpringConfiguration>

# IdP User Authentication

How to do it the v3 way?



# SWITCH

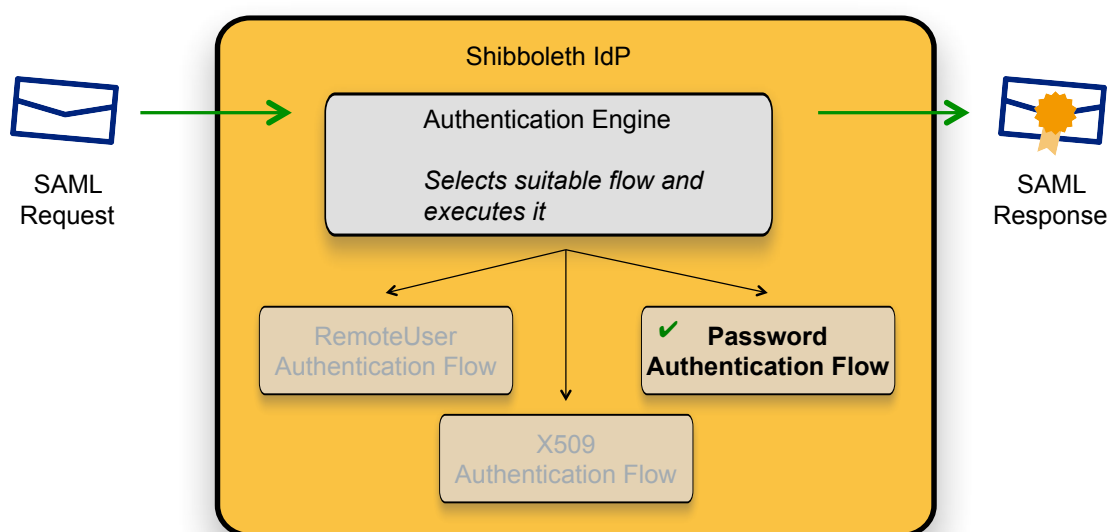
SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)



# From Login Handlers to Login Flows

- v2 uses "Login Handlers"
  - Typical/default setup: "UsernamePassword" login handler
    - Username/password login form
    - Authentication via JAAS and LDAP ("login.config")
  - Additional login handlers are available built-in (e.g. "RemoteUser") or as extension (e.g. "X.509", "Kerberos (SPNEGO)")
- v3 uses "Login Flows" (also called "Authentication Flows")
  - Typical/default setup: "Password" login flow
    - Username/password login form
    - Authentication via LDAP (natively), JAAS or Kerberos (username/password)
  - Additional login flows are available built-in (e.g. "RemoteUser", "X509"). A login flow for "SPNEGO/Kerberos" is in development.

## Login Flows



## Login Flows

- One or several flows can be activated.
- The authentication engine of the IdP selects a suitable flow depending on several criteria:
  - Does the SP request a specific authentication context type?
  - Does the SP request forced authentication?
  - Does the SP request passive authentication
- In practice, most deployments will use the "Password" login flow as the only one.
- ECP is supported out-of-the-box by the "Password" login flow. No special configuration is required.
  - But: Client must support ECP appropriately.

## Authentication Configuration

- Login flow activation:
  - `/opt/shibboleth-idp/conf/idp.properties:`

The active flows are specified via a regular expression (i.e. the order doesn't matter):

```
idp.authn.flows = Password
#idp.authn.flows = X509|Password
```

- Per login flow configuration:
  - `/opt/shibboleth-idp/conf/authn/*-config.xml`
- Side note: If multiple flows are activated, the order of the flows as defined in `conf/authn/general-authn.xml` might influence the flow selection process.

## Configuration: Username/password with LDAP

- Most deployments use this authentication mechanism.
- Login flow for username/password authentication:  
"Password" (activated by default)
- Configuration is done in two properties files:
  - All LDAP parameters, except credentials:  
`/opt/shibboleth-idp/conf/ldap.properties`
  - Credentials are stored separately (for security reasons):  
`/opt/shibboleth-idp/conf/credentials.properties`
- The properties of the LDAP authentication can be re-used for the LDAP configuration of the attribute resolution (all defined in `ldap.properties`).

## Example Configuration

- `/opt/shibboleth-idp/conf/ldap.properties`  
  

```
idp.authn.LDAP.authenticator = bindSearchAuthenticator
idp.authn.LDAP.ldapURL       = ldaps://ldap-test2.aai.switch.ch:636
idp.authn.LDAP.useStartTLS   = false
idp.authn.LDAP.useSSL        = true
idp.authn.LDAP.sslConfig     = jvmTrust
idp.authn.LDAP.baseDN        = ou=People,dc=example,dc=org
idp.authn.LDAP.subtreeSearch = true
idp.authn.LDAP.userFilter    = (uid={user})
idp.authn.LDAP.bindDN        = cn=idp,dc=example,dc=org
```
- `/opt/shibboleth-idp/conf/credentials.properties`  
  

```
[...]
idp.authn.LDAP.bindDNCredential = secret
[...]
```

## Properties for LDAP authentication

- General options
  - **idp.authn.LDAP.authenticator**  
User lookup and authentication method. Must be set to "bindSearchAuthenticator".
- Connection options
  - **idp.authn.LDAP.ldapURL**  
URL of the LDAP server(s). Must start with ldap:// or ldaps://. (Multiple servers can be specified by listing multiple URLs, separated by spaces)
  - **idp.authn.LDAP.useStartTLS**  
Enable TLS encryption for ldap:// URLs (port 389) (if not enabled, the connection is not encrypted).
  - **idp.authn.LDAP.useSSL:**  
Enable TLS encryption for ldaps:// URLs (port 636). Must usually be set to "true".

## Properties for LDAP authentication

- Connection options (continued)
  - **idp.authn.LDAP.sslConfig**  
Type of X.509 certificate verification method. Usually set to "jvmTrust".
- User Directory options
  - **idp.authn.LDAP.baseDN**  
Entry point in user directory
  - **idp.authn.LDAP.subtreeSearch**  
Enable searching the whole tree. Usually set to "true".
  - **idp.authn.LDAP.userFilter**  
LDAP search filter. Takes the login name as input.

## Properties for LDAP authentication

- LDAP service user options  
(The IdP connects to the LDAP server as this user to search for users.)
  - `idp.authn.LDAP.bindDN`  
Bind DN of the IdP service user
  - `idp.authn.LDAP.bindDNCredential`  
Password of the IdP service user

(Further properties for LDAP are available, but not described here. See the documentation for details.)

## Hands-on 1: Explore the configuration



### Get familiar with properties files:

- Which flows are enabled in  
`/opt/shibboleth-idp/conf/idp.properties`?  
(Hint: "idp.authn.flows")
- `/opt/shibboleth-idp/conf/ldap.properties`:
  - Which LDAP attribute holds the user's login name?
  - Which is the "Distinguished Name" (DN) of the service user the IdP uses for connecting to the LDAP server?
- Where is the password of the service user defined?

## Hands-on 1: Solutions

- Enabled flows: "Password"  
`idp.authn.flows = Password`
- LDAP attribute holding the login name: "uid"  
`idp.authn.LDAP.userFilter = (uid={user})`
- DN of the service user the IdP searches users with:  
`cn=idp,dc=example,dc=org`
- In the file  
`/opt/shibboleth-idp/conf/credentials.properties`  
`(idp.authn.LDAP.bindDNCredential = secret)`

## Hands-on 2: Migrate LDAP configuration from IdPv2



From IdPv2:

File `/opt/shibboleth-idp/conf/login.config`:

```
ShibUserPassAuth {  
    edu.vt.middleware.ldap.jaas.LdapLoginModule required  
        ldapUrl="ldaps://ldap-test1.aai.switch.ch:636 ldaps://ldap-test2.aai.switch.ch:636"  
        baseDn="ou=People,dc=example,dc=org"  
        bindDn="cn=idp,dc=example,dc=org"  
        bindCredential="secret"  
        userField="uid"  
        subtreeSearch="true";  
};
```

PS: Common and equivalent alternative to `userField`: `userFilter`

`UserField="uid" ⇔ userFilter="uid={0}"`

## Hands-on 2: Migrate LDAP configuration from IdPv2 (Hints)



```
ShibUserPassAuth {  
    edu.vt.middleware.ldap.jaas.LdapLoginModule required  
        ldapUrl="ldaps://ldap-test1.aai.switch.ch:636 ldaps://ldap-test2.aai.switch.ch:636"  
        baseDn="ou=People,dc=example,dc=org"  
        bindDn="cn=idp,dc=example,dc=org"  
        bindCredential="secret"  
        userField="uid"  
        subtreeSearch="true";  
};
```



- Edit `/opt/shibboleth-idp/conf/ldap.properties` and modify the property `idp.authn.LDAP.ldapURL`
- Restart Tomcat:  
`service tomcat7 restart`
- Test in browser

## Hands-on 2: Solution

To IdPv3:

File `/opt/shibboleth-idp/conf/ldap.properties`:

```
[...]  
idp.authn.LDAP.authenticator = bindSearchAuthenticator  
idp.authn.LDAP.ldapURL      = ldaps://ldap-test1.aai.switch.ch:636 \  
                             ldaps://ldap-test2.aai.switch.ch:636  
  
idp.authn.LDAP.useStartTLS  = false  
idp.authn.LDAP.useSSL      = true  
idp.authn.LDAP.sslConfig   = jvmTrust  
idp.authn.LDAP.baseDN      = ou=People,dc=example,dc=org  
idp.authn.LDAP.subtreeSearch = true  
idp.authn.LDAP.userFilter   = (uid={user})  
idp.authn.LDAP.bindDN      = cn=idp,dc=example,dc=org  
[...]
```

File `/opt/shibboleth-idp/conf/credentials.properties`:

```
[...]  
idp.authn.LDAP.bindDNCredential = secret  
[...]
```

## Advanced Topics

- JAAS authentication, as used in v2, is still supported in v3
  - Supported by the "Password" login flow. Needs to be activated in `/opt/shibboleth-idp/conf/authn/password-authn-config.xml`
  - JAAS configuration file (corresponds to login.config):  
`/opt/shibboleth-idp/conf/authn/jaas.config`
  - JAAS authentication is recommended for:
    - Connecting to multiple LDAP trees with different user bases
      - Might be done with native LDAP authentication, but requires complex configuration.
    - Connecting to other user directories like RDBMs (using specific JAAS module)
  - See the documentation on the Shibboleth wiki for details.

## References

### Documentation

- **Authentication Configuration**  
<https://wiki.shibboleth.net/confluence/display/IDP30/AuthenticationConfiguration>
- **Password Authentication Configuration**  
<https://wiki.shibboleth.net/confluence/display/IDP30/PasswordAuthnConfiguration>
- **Password / LDAP Authentication Configuration**  
<https://wiki.shibboleth.net/confluence/display/IDP30/LDAPAuthnConfiguration>
- **Advanced LDAP Configuration**  
<http://www.ldaptive.org/docs/guide/authentication>
- **Password / JAAS Authentication Configuration**  
<https://wiki.shibboleth.net/confluence/display/IDP30/JAASAuthnConfiguration>



# IdP Login Form Customization

Templates and Customization



# SWITCH

SWITCHaai Team

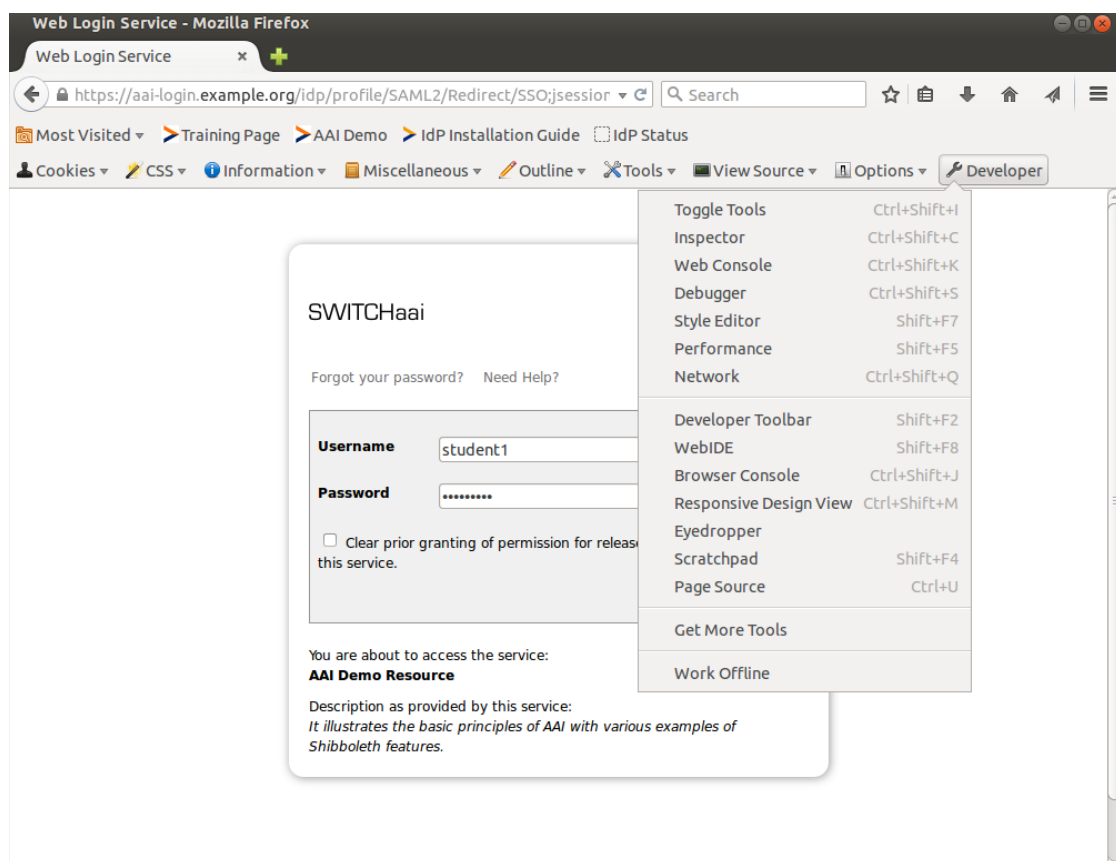
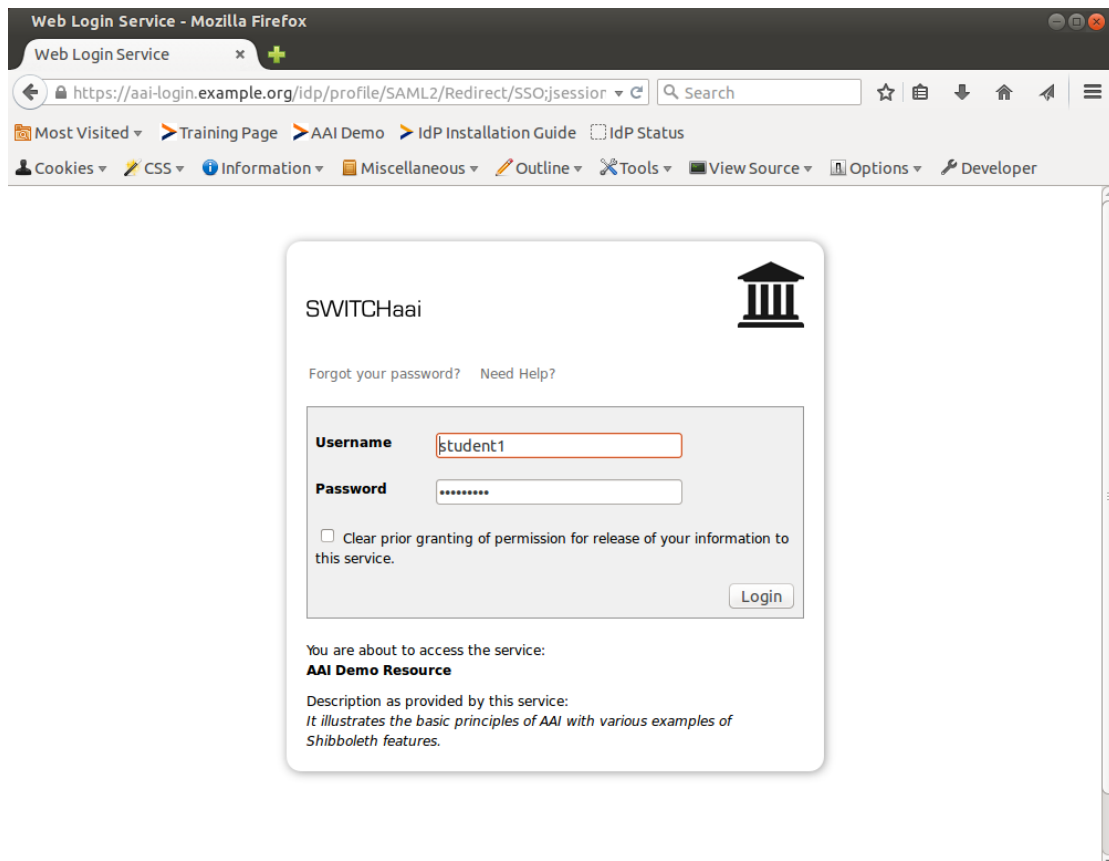
[aai@switch.ch](mailto:aai@switch.ch)

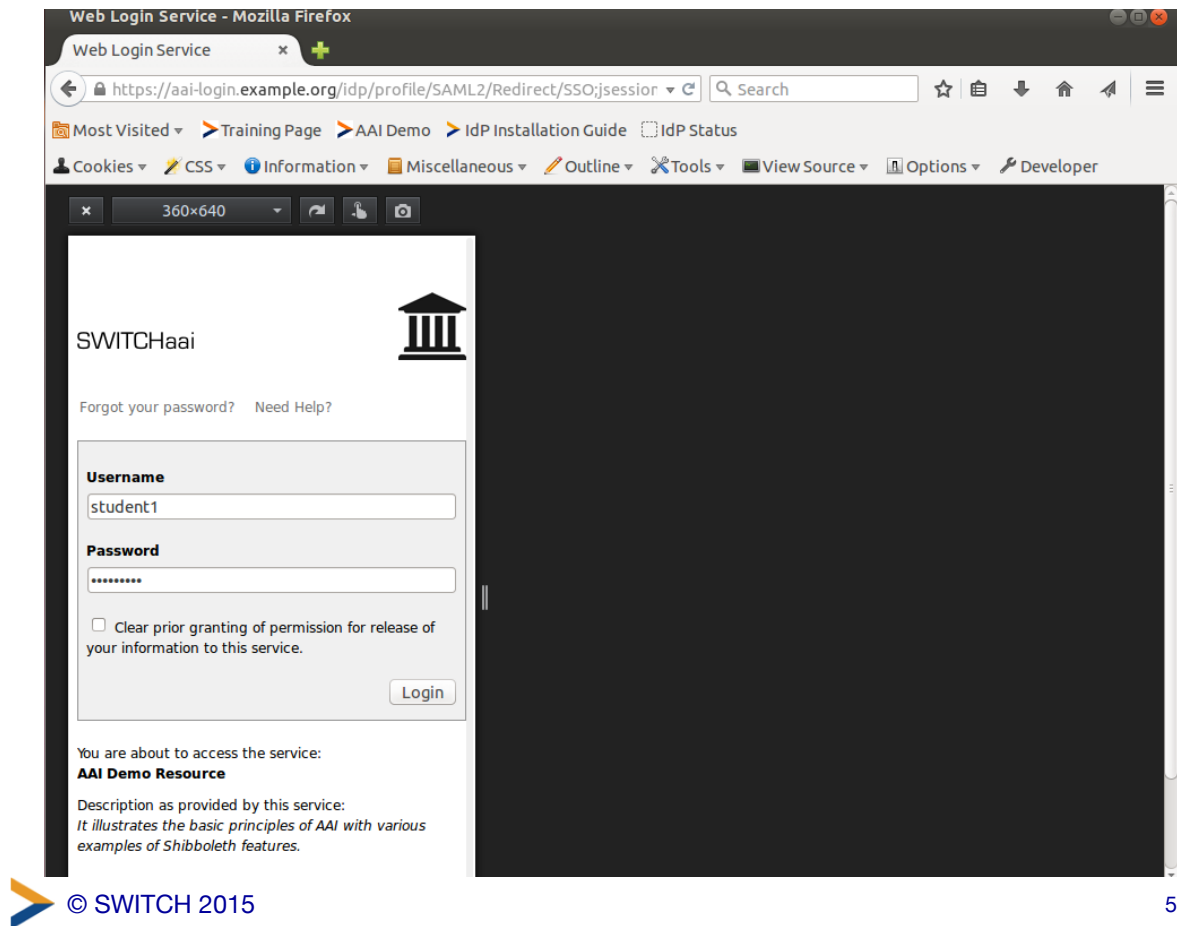
 © SWITCH 2015

## Overview

- How to
  - Customize look and feel
  - Customize messages/languages
  - Add text to your login site

 © SWITCH 2015





5

## Layout

- Change the look and feel in  
/opt/shibboleth-idp/edit-webapp  
(images and css)
- Place additional web resources in the edit-webapp directory, not the webapp directory. The webapp directory is replaced upon every IdP upgrade.
- Rebuild the idp.war file and restart tomcat

6

# Spring message properties

- in `/opt/shibboleth-idp/messages` you find
  - `authn-messages.properties`
  - `error-messages.properties`
  - `consent-messages.properties`these messages are used in the velocity template
- internationalization:
  - `consent-messages_de.properties`
  - `consent-messages_fr.properties` etc.

## error-messages.properties

in `/opt/shibboleth-idp/messages/error-messages.properties`

# General strings

`idp.title = Web Login Service`

`idp.title.suffix = Error`

`idp.logo = /images/example.org.png`

`idp.logo.alt-text = Example Home Organisation`

`idp.logo.target.url = http://www.example.org`

`idp.message = An unidentified error occurred.`

`idp.footer = Insert your footer text here.`

# Error key to title and message mappings

`unexpected.title = Unexpected Error`

`unexpected.message = An unexpected error was encountered, usually reflecting a configuration or software error.`

# authn-messages.properties

in /opt/shibboleth-idp/messages/authn-messages.properties

```
idp.login.loginTo = Login to
idp.login.username = Username
idp.login.password = Password
idp.login.donotcache = Don't Remember Login
idp.login.login = Login
idp.login.forgotPassword = Forgot your password?
idp.login.forgotPassword.url = https://support.example.org
idp.login.needHelp = Need Help?
```


# authn-messages.properties

in /opt/shibboleth-idp/messages/authn-messages.properties

```
# Classified Login Error messages
UnknownUsername = bad-username
InvalidPassword = bad-password
ExpiredPassword = expired-password
AccountLocked = account-locked
bad-username.message = The username you entered cannot be identified.
bad-password.message = The password you entered was incorrect.
expired-password.message = Your password has expired.
account-locked.message = Your account is locked.
```

# Velocity Properties

```
<a class="aai" href="#"
#springMessage("idp.login.forgotPassword.url")
">
#springMessageText("idp.login.forgotPassword",
"Forgot your password?")
</a>
```

SWITCHaai

[Forgot your password?](#) [Need Help?](#)

**Username**

student1

**Password**

\*\*\*\*\*

☐ Clear prior granting of permission for release of your information to this service.

Login

**Technical support:**  
E-Mail: [Helpdesk](#)  
Phone (internal): 9   
Phone (external): +41   
IT Services: [IT Services Webpage](#)

You are about to access the service:

**AAI Demo Resource**  
Description as provided by this service:  
*It illustrates the basic principles of AAI with various examples of Shibboleth features.*

# Velocity

- The Apache Velocity Engine is a free open-source templating engine.
- clean separation between the presentation tier and business tiers
- VTL (Velocity Template Language)
  - References begin with \$
  - Directives begin with #
  - A single line comment begins with ## and finishes at the end of the line.
  - Multi-line comments, which begin with #\* and end with \*#

## Login and intercept

- The velocity templates are under `/opt/shibboleth-idp/views`
  - `login.vm`
  - `login-error.vm`
  - `intercept/attribute-release.vm`
  - `intercept/terms-of-use.vm`
  - `error.vm`are most used (no restart required)
- Additional custom pages can be added , e.g. for expiring passwords, locked accounts etc.

## Some Velocity Properties

- `$rpUIContext.informationURL`
- `$rpUIContext.logo`
- `$rpUIContext.organizationDisplayName`
- `$rpUIContext.organizationName`
- `$rpUIContext.organizationURL`
- `$rpUIContext.privacyStatementURL`
- `$rpUIContext.serviceDescription`
- `$rpUIContext.serviceName`

## Velocity Properties

```
#set ($name = $rpUIContext.serviceName)
#if ($name)
  <div class="space">
    <em>$encoder.encodeForHTML($name)</em>
  </div>
#end
```



## Hands On I - III

- change the background-color of the class `.aai_login_field` from grey to any other color
- return the following error message on the login form in case of invalid username or incorrect password:  
  
“ The credentials you entered are incorrect.”
- Start to adapt the `login.vm` in such way that it looks like your production IdP.

## Example Solution I

- change the background-color in `aai_login_field` class in `/opt/shibboleth-idp/edit-webapp/css/main.css`  
  

```
.aai_login_field { ...  
    background-color: #4EEE94;  
    ... }
```
- rebuild and restart tomcat  

```
sudo JAVACMD=/usr/bin/java /opt/shibboleth-idp/bin/  
    build.sh -Didp.target.dir=/opt/shibboleth-idp  
sudo /etc/init.d/tomcat7 restart
```
- might be you need to reload linked stylesheets in the browser to see the effect

## Example Solution II

- Edit authn-messages.properties

UnknownUsername = bad-credentials

InvalidPassword = bad-credentials

bad-credentials.message = The credentials  
you entered are incorrect.

## IdP Attribute Resolution

### Migrating configuration to version 3



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Attribute processing in IdP version 3

1. Resolution
2. Filtering
3. Encoding

## Compatibility with version 2

- Same XML syntax as v2, should be "nearly 100% compatible"  
Any regression should be reported as a bug
- Some deprecated elements are ignored
- **Exception:** scripted attribute definitions  
Deprecated interfaces may require complex scripts to be adapted

## Why upgrade your configuration?

- No warning for using legacy configuration mode
- Delete ignored elements
- Grouping attribute definitions in separate files

⇒ Less misleading, smaller files, clearer

## Deprecated items

- Principal connectors
- NameID encoders
- Transient identifier attribute definitions
- Persistent identifier data connectors and attribute definitions

All replaced by NameID generation/consumption, see next presentation

## New features in version 3

- Property replacement: `%{my.property}`
  - Move passwords in a dedicated file
  - Extract duplicated data like URLs
- Can split configuration into several files
- External Spring configuration for data connectors
- Activation conditions on attribute encoders, attribute definitions and data connectors

## New features example

```
<resolver:DataConnector id="myStoredId"
  xsi:type="dc:StoredId"
  generatedAttributeID="persistentID"
  sourceAttributeID="%{idp.persistentId.sourceAttribute}"
  salt="%{idp.persistentId.salt}"
  queryTimeout="0">
  <resolver:Dependency ref="%{idp.persistentId.sourceAttribute}" />
  <dc:BeanManagedConnection>
    shibboleth.PostgreSQLDataSource
  </dc:BeanManagedConnection>
</resolver:DataConnector>
```

```
<resolver:DataConnector id="myLDAP" xsi:type="dc:LDAPDirectory"
  ldapURL="%{idp.attribute.resolver.LDAP.ldapURL}"
  baseDN="%{idp.attribute.resolver.LDAP.baseDN}"
  principal="%{idp.attribute.resolver.LDAP.bindDN}"
  principalCredential="%{idp.attribute.resolver.LDAP.bindDNCredential}"
  useStartTLS="%{idp.attribute.resolver.LDAP.useStartTLS:true}">
  <dc:FilterTemplate>%{idp.attribute.resolver.LDAP.searchFilter}</dc:Fi
  <!-- actual values come from conf/ldap.properties -->
</resolver:DataConnector>
```



# Hands-on 1

Add a new local attribute definition and release it to the attribute viewer.

```
UZH SAP user ID
SAP User ID used internally by University of Zürich
SAML1 Name: urn:mace:unizh.ch:uzhSapUserId
SAML2 Name: urn:oid:1.3.6.1.4.1.11817.1.1.2.13
Friendly name: uzhSAPUserId
Format: SAP-<username>
```

source: [Resource Registry](#)

([https://rr.aai.switch.ch/list\\_attributes.php?sort=name](https://rr.aai.switch.ch/list_attributes.php?sort=name))



# Hands-on 1 solution

## attribute-resolver-local.xml

New file with:

```
<resolver:AttributeDefinition id="uzhSAPUserId" xsi:type="ad:Template">
  <resolver:Dependency ref="uid" />
  <resolver:AttributeEncoder xsi:type="enc:SAML1String"
    name="urn:mace:unizh.ch:uzhSapUserId" encodeType="false" />
  <resolver:AttributeEncoder xsi:type="enc:SAML2String"
    name="urn:oid:1.3.6.1.4.1.11817.1.1.2.13"
    friendlyName="uzhSAPUserId" encodeType="false" />
  <ad:Template>SAP-{$uid}</ad:Template>
  <ad:SourceAttribute>uid</ad:SourceAttribute>
</resolver:AttributeDefinition>
```



# Hands-on 1 solution

## attribute-filter-local.xml

New file with:

```
<afp:AttributeFilterPolicy id="uzhSAPUserId">
  <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
    value="https://attribute-viewer.aai.switch.ch/shibboleth" />
  <afp:AttributeRule attributeID="uzhSAPUserId">
    <afp:PermitValueRule xsi:type="basic:ANY" />
  </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

Doable in Resource Registry too



# Hands-on 1 solution

## services.xml

Loads both new files:

```
<util:list id="shibboleth.AttributeResolverResources">
  <value>${idp.home}/conf/attribute-resolver-switchaai-core.xml</value>
  <value>${idp.home}/conf/attribute-resolver-connectors.xml</value>
  <value>${idp.home}/conf/attribute-resolver-other.xml</value>
  <value>${idp.home}/conf/attribute-resolver-local.xml</value>
</util:list>
```

```
<util:list id="shibboleth.AttributeFilterResources">
  <ref bean="FileBackedSWITCHAaiAttributeFilter" />
  <value>${idp.home}/conf/attribute-filter-local.xml</value>
</util:list>
```

## ScriptedAttribute differences

- IdP API for scripts has changed
  - output attribute variable already created
  - `setValues()` removed
  - and more, see [ScriptedAttributeDefinition](https://wiki.shibboleth.net/confluence/display/IDP30/ScriptedAttribute) (<https://wiki.shibboleth.net/confluence/display/IDP30/ScriptedAttribute> for details)
- Alternatives: mapped or template attribute definitions
- JavaScript engine change between Java 7 (Rhino) and 8 (Nashorn) ⇒ even *more* things to adapt

## Mapped attribute definition

- Many-to-many mapping from source attributes values
- Each input value is checked against every mapping if match → input replaced by return value
- Supports regular expressions
- One or more mapping statements: `ValueMap`
  - one `ReturnValue`
  - one or more `SourceValue`
- Zero or one `DefaultValue`, fixed or pass-through



## Mapped attribute example

```
<resolver:AttributeDefinition id="eduPersonAffiliation"
  xsi:type="ad:Mapped" sourceAttributeID="eduPersonAffiliation">
  <!-- common attributes omitted -->
  <ad:DefaultValue passThru="true"/>
  <ad:ValueMap>
    <ad:ReturnValue>member</ad:ReturnValue>
    <ad:SourceValue>staff|student|faculty|employee</ad:SourceValue>
  </ad:ValueMap>
  <ad:ValueMap>
    <ad:ReturnValue>$1</ad:ReturnValue>
    <ad:SourceValue>(staff|student|faculty|employee)</ad:SourceValue>
  </ad:ValueMap>
</resolver:AttributeDefinition>
```

- student → student, member
- alumni → alumni

## Template attribute definition

- Combines values of multiple input attributes
- Velocity template
- **All** input attributes must contain the **same number** of values
- Zero or one Template
- One or more SourceAttribute

# Template attribute example

```
<resolver:AttributeDefinition id="template" xsi:type="ad:Template">
  <resolver:Dependency ref="OtherAttribute" />
  <resolver:Dependency ref="myLdap" />
  <!-- common attributes omitted -->
  <ad:Template>${attrFromLdap}::${OtherAttr}</ad:Template>
  <ad:SourceAttribute>attrFromLdap</ad:SourceAttribute>
  <ad:SourceAttribute>OtherAttr</ad:SourceAttribute>
</resolver:AttributeDefinition>
```

- ldap1, other1 → ldap1::other1
- ldap1, ldap2, other1 → error!



## Hands-on 2

Add new eduPersonEntitlement values of the form `https://example.org/groups/<objectClass>` using the LDAP `objectClass` attribute, *without* using script attributes



## Hands-on 2 solution

Create a new template attribute definition (without encoders) to generate the new values:

```
<resolver:AttributeDefinition id="eduPersonEntitlement.groups"
  xsi:type="ad:Template" sourceAttributeID="objectClass" dependencyOnly
  <resolver:Dependency ref="myLDAP" />
  <ad:Template>https://example.org/groups/${objectClass}</ad:Template>
  <ad:SourceAttribute>objectClass</ad:SourceAttribute>
</resolver:AttributeDefinition>
```

Add that new attribute to the definition of eduPersonEntitlement:

```
<resolver:AttributeDefinition id="eduPersonEntitlement" xsi:type="ad:Si
  <resolver:Dependency ref="eduPersonEntitlement.common-lib-terms" />
  <resolver:Dependency ref="eduPersonEntitlement.groups" />
  <!-- ... rest of original definition -->
</resolver:AttributeDefinition>
```

## References

- Shibboleth wiki: [AttributeResolverConfiguration](https://wiki.shibboleth.net/confluence/display/IDP30/AttributeResolverConfiguration)  
(<https://wiki.shibboleth.net/confluence/display/IDP30/AttributeResolverConfiguration>) and its child pages
- Shibboleth wiki: [AttributeFilterConfiguration](https://wiki.shibboleth.net/confluence/display/IDP30/AttributeFilterConfiguration)  
(<https://wiki.shibboleth.net/confluence/display/IDP30/AttributeFilterConfiguration>)
- Shibboleth wiki: [AttributeDefinitionConfiguration](https://wiki.shibboleth.net/confluence/display/IDP30/AttributeDefinitionConfiguration)  
(<https://wiki.shibboleth.net/confluence/display/IDP30/AttributeDefinitionConfiguration>) and its child pages
- Rhino Migration Guide  
(<https://wiki.openjdk.java.net/display/Nashorn/Rhino+Migration+Guide>)

# IdP Persistent IDs

## Configuration changes and database migration



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Persistent IDs in SAML – short recap

- a *persistent, revocable, non-reassignable, opaque, targeted, non-global* identifier for identifying the subject in a SAML assertion  
[<https://wiki.shibboleth.net/confluence/display/CONCEPT/NameIdentifiers>]
- introduced in 2005 with the SAML V2.0 specification:  
*"Persistent name identifiers generated by identity providers MUST be constructed using pseudo-random values that have no discernible correspondence with the subject's actual identifier (for example, username). The intent is to create a non-public, pair-wise pseudonym to prevent the discovery of the subject's identity or activities."*
- first implemented in the Shibboleth IdP 2; full-featured persistent ID support requires a database
- configuration instructions included in the SWITCH IdP deployment guide since 2008, with MySQL as the suggested backend

# Persistent IDs in practice

- on the wire (in a SAML assertion)

```
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
NameQualifier="https://aai-login.example.org/idp/shibboleth"
SPNameQualifier="https://sp.example.org/shibboleth">jQ+KQZR4OHyNi9702/
kW5KIQFhk=</NameID>
```

- attribute rendering in the Shibboleth SP (string)

```
https://aai-login.example.org/idp/shibboleth!https://sp.example.org/
shibboleth!jQ+KQZR4OHyNi9702/kW5KIQFhk=
```

- by default, the Shibboleth IdP creates the persistent ID proper by calculating the SHA-1 hash of the SP's entity ID plus a user attribute value plus an admin-specified salt (i.e., the output is 20 bytes, Base64 encoded)
- when used in a federation, always qualified by the IdP and SP entity IDs

# Persistent ID changes with the IdP v3

- no disruptive ones, but a couple of things have happened behind the scenes
- most importantly, the IdP v3 brings a **new, dedicated NameID generation service**
  - preferred over the previous method available in v2, which treated name IDs as a sort of “special-purpose” attributes
  - deprecates the `storedId` data connector and the `SAML2NameID` attribute definition type
  - in a pure v3 configuration and an ideal SAML 2 world, the IdP would only include NameIDs in the `<Subject>` element of an assertion
  - the configuration in the v3 SWITCH deployment guide has been updated to the new-style generation as far as possible, but still allows encoding of persistent IDs in SAML attributes

# Configuring the NameID generation service

- configure the parameters for the service in

**/opt/shibboleth-idp/conf/saml-nameid.properties:**

```
idp.persistentId.generator = shibboleth.StoredPersistentIdGenerator
idp.persistentId.store = PersistentIdStore
idp.persistentId.sourceAttribute = swissEduPersonUniqueID.withoutAttributeEncoder
```

- to enable the generating side of the service, remove the comments around the `shibboleth.SAML2PersistentGenerator` bean reference in `/opt/shibboleth-idp/conf/saml-nameid.xml`
- to support the reverse mapping (from a persistent ID back to a user), remove the comments around the `c14n/SAML2Persistent` bean reference in `/opt/shibboleth-idp/conf/c14n/subject-c14n.xml`
- finally, add the proper `idp.persistentId.salt` value to `/opt/shibboleth-idp/conf/credentials.properties` (carry over from your v2 configuration)

## Retaining persistent IDs from your v2 IdP

- the database schema for the `shibpid` table remains unchanged
- when setting up a new IdP v3 from scratch, SWITCH recommends PostgreSQL as the database backend (unless relying on an existing, separately hosted RDBMS)
- “transferring” the records from MySQL to PostgreSQL is straightforward:

```
me@idpv2$ sudo mysqldump --compatible postgres --compact --no-create-info
--result-file shibpid.sql shibboleth shibpid
me@idpv3$ sudo -iu postgres psql shibboleth --file /path/to/shibpid.sql
```

- make sure to import the records into an empty table, i.e. execute `sudo -u postgres psql shibboleth -c "truncate shibpid"` before importing a newer version of a full dump



## (Some ideas for) hands-on exercises

- examine the current contents of the `shibpid` table:  

```
$ sudo -iu postgres psql shibboleth
shibboleth=# \pset pager off
shibboleth=# \dS shibpid
shibboleth=# select * from shibpid;
```
- delete a record from the `shibpid` table, and “recreate” it by logging in again with the respective account (on the proper SP)
- dump the `shibpid` table to a file, purge the table with truncate, and reimport the records
- log in to your v2 [test] IdP, figure out the current number of `shibpid` records, and make a dump of that table

## IdP User Consent

Transparency for attribute release



# SWITCH

SWITCHaai Team  
aai@switch.ch

# **Part 1: Overview of user consent in IdP version 3**

## **Part 2: Technical bits**

## **User consent**

### **Two pieces**

1. Attribute release consent [enabled]
2. Terms of use consent [disabled]

Both prompt user on first access to every SP and again when attributes or terms change.



## What's in version 3

- Attribute release and terms of use consent now built in
- Inspired by uApprove and uApproveJP plugins for v2
- No consent data migration, storage implementations are *not compatible*
- May be enabled or disabled per relying party and per profile
- Decisions logged

## Differences with uApprove

- User can select attributes to release [disabled]
- Consent duration choices
  1. "Ask me again if information changes"  
= if *set* of attributes changes
  2. "Ask me again at next login" [enabled]
  3. "Do not ask me again", ever, for any SP [enabled]
- No regular expression for SP white/black lists
- No translations provided

## Why enable user consent?

- Easier to have now with v3 than with v2
- Required by SWITCHaai Interfederation Access Declaration
- Inform users about what personal data is transmitted in a more real-time fashion
- Recommended to comply with data protection laws

## Why (not) enable user consent?

- One more page to read and click through upon login, but only the first time for each SP
- Global consent disabled: users cannot choose "I don't care about my privacy"
- Decide for all your users or let them decide?

## When should consent be sought?

- All SPs: the best option ← recommended
- Outside your organisation: good, less clicks
- Outside CH: currently no technical means to distinguish "Swiss" SPs and the data might not even be stored in Switzerland

## Part 2: Technical bits

# Global configuration options

Configured by Spring beans in `conf/relying-party.xml`, see comments inside for overrides

## Post-authentication flows

- Attribute consent [enabled]
- Terms of use consent [disabled]

# Example `conf/relying-party.xml`

Both post-authentication flows enabled for SAML2 SSO  
[only attribute-release]

```
<bean id="shibboleth.DefaultRelyingParty" parent="RelyingParty">
  <property name="profileConfigurations">
    <list>
      <bean parent="Shibboleth.SSO"
        p:postAuthenticationFlows="attribute-release" />
      <ref bean="SAML1.AttributeQuery" />
      <ref bean="SAML1.ArtifactResolution" />
      <bean parent="SAML2.SSO"
        p:postAuthenticationFlows="#{'terms-of-use','attribute-release'}"/>
      <ref bean="SAML2.ECP" />
      <ref bean="SAML2.Logout" />
      <ref bean="SAML2.AttributeQuery" />
      <ref bean="SAML2.ArtifactResolution" />
    </list>
  </property>
</bean>
```

# Attribute consent configuration

Configured by Java properties in  
`conf/idp.properties`

## Consent duration options

- "Ask me again if information changes"  
Always available to users
- "Ask me again at next login"  
`idp.consent.allowDoNotRemember = true`  
[true]
- "Do not ask me again"  
`idp.consent.allowGlobal = false` [true]

# Attribute consent configuration

## Per attribute behaviour

- Allow selection of attributes to release, may break applications if required attributes are withheld  
`idp.consent.allowPerAttribute = false`  
[false]
- Ask again if attribute *values* change  
`idp.consent.compareValues = true` [false]

# Intercept flow configuration

Configured by Spring beans in  
`conf/intercept/consent-intercept-  
config.xml`

## White & black lists

Which attribute to prompt for [all except black list]

- White list [empty]  
**When filled:** any attribute not mentioned in a list is released *without asking*
- Black list [`transientId`, `persistentId`,  
`eduPersonTargetedID`]
- Pattern match [not defined]

# Intercept flow configuration

## Attribute display order (coming in version 3.2.0)

- Alphabetical order by default
- Except attributes in white list show up first
- Set pattern to `^.*$` to catch all other attributes
- Fully customised order ⇒ implement  
`java.util.Comparator<String>`

# Terms of use consent configuration

Configured by Java properties in `messages/consent-messages.properties`

## Terms for each SP

- Default mapping using the `entityID`

```
https\://sp.example.org = example-tou-1
example-tou-1.title = Example Terms of Use
example-tou-1.text = <em>This is an example ToU</em> [...]
```

- Other mapping configurable but the key is still `entityID` (default value available)

# Custom terms of use mapping

Configured by Spring beans in `conf/intercept/consent-intercept-config.xml`

Provided bean mapping `entityIDs` to values [disabled]

```
<bean id="shibboleth.consent.terms-of-use.Key"
      class="com.google.common.base.Functions" factory-method="compose">
  <constructor-arg name="g">
    <bean class="com.google.common.base.Functions" factory-method="forMap"
          c:defaultValue="terms-of-use">
      <constructor-arg name="map">
        <map>
          <entry key="https://sp.example.org/shibboleth" value="example-terms" />
        </map>
      </constructor-arg>
    </bean>
  </constructor-arg>
  <constructor-arg name="f">
    <ref bean="shibboleth.RelyingPartyIdLookup.Simple" />
  </constructor-arg>
</bean>
```



## Hands-on: use only one ToU

We want to always display the same terms of use regardless of the SP.



## Hands-on solution

- Enable terms-of-use flow in conf/relying-party.xml
- Change key bean in conf/intercept/consent-intercept-config.xml to

```
<bean id="shibboleth.consent.terms-of-use.Key"
      class="com.google.common.base.Functions"
      factory-method="constant">
  <constructor-arg value="my-terms" />
</bean>
```





## Hands-on solution

- Add text in messages/consent-messages.properties

```
my-terms = bogus-tou
bogus-tou.title = Bogus Terms of Use
bogus-tou.text = You can do anything you want!
```

## References

- Shibboleth wiki: [ConsentConfiguration](https://wiki.shibboleth.net/confluence/display/IDP30/ConsentConfiguration)  
(<https://wiki.shibboleth.net/confluence/display/IDP30/ConsentConfiguration>)
- Shibboleth wiki: [RelyingPartyConfiguration](https://wiki.shibboleth.net/confluence/display/IDP30/RelyingPartyConfiguration)  
(<https://wiki.shibboleth.net/confluence/display/IDP30/RelyingPartyConfiguration>)
- Google Guava [Functions](http://docs.guava-libraries.googlecode.com/git/javadoc/com/google/common/base/Function) class Javadoc  
(<http://docs.guava-libraries.googlecode.com/git/javadoc/com/google/common/base/Function>)

## Appendix: Disabling attribute consent prompt for particular SPs

## Disabling prompt for particular SPs

### Relying party overrides

- Template beans in `conf/relying-party.xml` to match SPs by:
  - name: `entityID`
  - group: `<EntitiesDescriptor>` in metadata
  - tag: `<EntityAttributes>` metadata extension
- **First match wins** ⇒ order in `conf/relying-party.xml` is significant

# Disabling prompt for particular SPs

## Entity attributes in metadata

- Entity categories
  - GÉANT Data Protection Code of Conduct (CoCo)
  - REFEDS Research & Scholarship
- New attributes available!
  - swissEduPersonHomeOrganization
  - swissEduPersonHomeOrganizationType

## Example metadata with attributes

```
<EntityDescriptor
  entityID="https://attribute-viewer.aai.switch.ch/interfederation-test/shibbol
  <Extensions>
    <mdattr:EntityAttributes>
      <saml:Attribute Name="http://macedir.org/entity-category">
        <saml:AttributeValue>
          http://www.geant.net/uri/dataprotection-code-of-conduct/v1
        </saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute FriendlyName="swissEduPersonHomeOrganization"
        Name="urn:oid:2.16.756.1.2.5.1.1.4">
        <saml:AttributeValue>switch.ch</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute FriendlyName="swissEduPersonHomeOrganizationType"
        Name="urn:oid:2.16.756.1.2.5.1.1.5">
        <saml:AttributeValue>others</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
  <!-- ... rest of metadata for entity -->
</EntityDescriptor>
```

# Example relying party override

Disables flows for SPs belonging to a home organisation

```
<util:list id="shibboleth.RelyingPartyOverrides">
  <!-- ... more beans -->
  <bean id="shibboleth.NoUserConsentRelyingParty" parent="RelyingPartyByTag">
    <constructor-arg name="candidates">
      <list>
        <bean id="disableForSingleHomeOrganization" parent="TagCandidate"
          c:name="urn:oid:2.16.756.1.2.5.1.1.4"
          p:values="example.org" />
        <!-- ... more beans -->
      </list>
    </constructor-arg>
    <property name="profileConfigurations">
      <list>
        <ref bean="Shibboleth.SSO" />
        <ref bean="SAML2.SSO" />
        <!-- ... other profiles -->
      </list>
    </property>
  </bean>
</util:list>
```

## IdP Upgrades within Version 3

It's easy now



# SWITCH

SWITCHaai Team  
aai@switch.ch

## The IdPv3 makes upgrading easy

*The upgrade process is designed to be very safe, and will never overwrite any configuration files, views/templates, properties, etc. that you have modified.*

**→ Keep your IdP up to date!**

## Upgrading

### Procedure:

- Download the latest Identity Provider software package.
- Unpack it at any convenient location (it won't be needed afterwards).
- Change into the newly created distribution directory.
- Upgrade the current deployment in `/opt/shibboleth-idp` by running the `install.sh` script.
- Review any necessary changes (e.g. based on the information from SWITCH or from the release notes).
- Run the `build.sh` script to re-build the warfile.
- Restart Tomcat to activate the new version.

**Detailed instructions are available in the installation guide:**

<https://www.switch.ch/aai/guides/idp/installation/#keepinguptodate>

## Good to know

- There are two distinct areas below `/opt/shibboleth-idp`:
  - *Unmanaged directories*  
Directories managed by you (not touched by upgrades),  
e.g. `conf/`, `views/`, `edit-webapp/`
  - *Managed directories*  
System directories managed by the IdP software  
(updated during upgrades), e.g. `system/`, `webapp/`
  - *Never touch the the system directories*  
`system/` and `webapp/`!
- Upgrades may introduce new features that require adaptations to the configuration to make use of these new features. But the existing configuration should still work without these changes.

## References

### Documentation

- **SWITCHaai IdPv3 Installation Guide, "Keeping up to date"**  
<https://www.switch.ch/aai/guides/idp/installation/#keepinguptodate>
- **Shibboleth Documentation**
  - **Upgrading**  
<https://wiki.shibboleth.net/confluence/display/IDP30/Upgrading>
  - **Release Notes**  
<https://wiki.shibboleth.net/confluence/display/IDP30/ReleaseNotes>

# IdP Updating the Home Organisation Description

## Changes in Resource Registry



# SWITCH

SWITCHaai Team  
aai@switch.ch

**What technically defines your  
Identity Provider in SWITCHaai or  
eduGAIN?**

**Its SAML2 Metadata**

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <EntityDescriptor
3   xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
4   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
6   xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
7   xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
8   xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
9   xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata saml-schema-metadata-2.0.xsd urn:mace:shibboleth:me
10  entityID="https://aai-logon.switch.ch/idp/shibboleth">
11   <Extensions>
12     <mdrpi:PublicationInfo
13       publisher="https://rr.aai.switch.ch/gen_saml2md_entity.php?objectType=homeOrg&objectID=130"
14       creationInstant="2015-06-05T13:58:52Z">
15     </mdrpi:PublicationInfo>
16     <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
17       <saml:Attribute Name="http://macedir.org/entity-category-support" NameFormat="urn:oasis:names:tc:SAML:2.
18       <saml:AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</saml:AttributeValue>
19       <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
20     </saml:Attribute>
21     </mdattr:EntityAttributes>
22   </Extensions>
23   <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:SAML:1
24   <Extensions>
25     <mdrpi:PublicationInfo
26       publisher="https://rr.aai.switch.ch/gen_saml2md_entity.php?objectType=homeOrg&objectID=130"
27       creationInstant="2015-06-05T13:58:52Z">
28     </mdrpi:PublicationInfo>
29     <shibmd:Scope regexp="false">switch.ch</shibmd:Scope>
30     <mdui:UIInfo>
31       <mdui:DisplayName xml:lang="de">SWITCH</mdui:DisplayName>
32       <mdui:DisplayName xml:lang="en">SWITCH</mdui:DisplayName>
33       <mdui:DisplayName xml:lang="fr">SWITCH</mdui:DisplayName>
34       <mdui:DisplayName xml:lang="it">SWITCH</mdui:DisplayName>
35       <mdui:Description xml:lang="de">SWITCH erbringt innovative, einzigartige Internet-Dienstleistungen für
36       <mdui:Description xml:lang="en">SWITCH provides innovative, unique internet services for the Swiss uni
37       <mdui:Description xml:lang="fr">SWITCH fournit des prestations innovantes et uniques pour les hautes é
38       <mdui:Description xml:lang="it">SWITCH eroga servizi Internet innovativi e unici per le scuole univers
39       <mdui:Keywords xml:lang="en">Zurich</mdui:Keywords>
40       <mdui:Keywords xml:lang="de">Zürich</mdui:Keywords>
41       <mdui:Keywords xml:lang="fr">Zurich</mdui:Keywords>
42       <mdui:Keywords xml:lang="it">Zurigo</mdui:Keywords>
43       <mdui:Logo height="16" width="16">data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAABAAAAAQCAYAAAAf8/9hA
44       <mdui:Logo height="60" width="80">data:image/png;base64,iVBORw0KGgoAAAANSUheUgAAAFAAAAA8CAYAAADxJz2MA
45       <mdui:InformationURL xml:lang="en">http://www.switch.ch/about/</mdui:InformationURL>
46       <mdui:InformationURL xml:lang="de">http://www.switch.ch/de/about/</mdui:InformationURL>
47       <mdui:InformationURL xml:lang="fr">http://www.switch.ch/fr/about/</mdui:InformationURL>
48       <mdui:InformationURL xml:lang="it">http://www.switch.ch/it/about/</mdui:InformationURL>
49     </mdui:UIInfo>
50     <mdui:DiscoHints>
51       <mdui:IPHint>130.59.0.0/16</mdui:IPHint>
52       <mdui:YPHint>2001:620::/48</mdui:YPHint>

```

3

## Does metadata change when IdP is upgraded?

No, but revising some parts of metadata still is recommended.



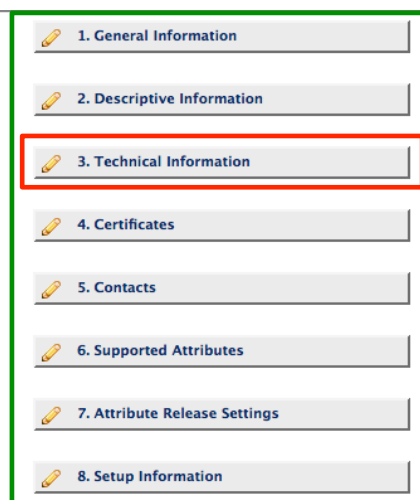
## IdPv2 vs IdPv3 Metadata

- **Endpoint URLs stay the same!** 😊
  - Unlike upgrade vom IdPv1 to IdPv2
  - Therefore, no metadata/Resource Registry change needed in general
- However, **some changes still recommended:**
  1. Review the Home Organisation Description
  2. Change URL for Attribute Authority
  3. Remove Unnecessary Endpoints
- To change metadata, **change Home Organisation description**
  - Apply change in AAI Resource Registry: <https://rr.aai.switch.ch>

## Home Organisation Description

### Home Organization Menu for 'SWITCH'

Change the following sections in order to modify this Home Organization Description. Please note that **any change becomes active** when the federation metadata is published the next time. This is usually the case on every full hour.




The screenshot shows a menu with eight items, each with a pencil icon and a text label. A green box highlights the first three items, and a red box highlights the third item.

|                               |
|-------------------------------|
| 1. General Information        |
| 2. Descriptive Information    |
| 3. Technical Information      |
| 4. Certificates               |
| 5. Contacts                   |
| 6. Supported Attributes       |
| 7. Attribute Release Settings |
| 8. Setup Information          |

**1./2. To review**

**3. To adapt**

 View Home Organization Description

# 1. Review the Home Organisation Description

In particular review and adapt if necessary:

## ■ 1. General Information

- Interfederation Support (option only available if Interfederation Access Declaration has been signed. More information on <https://www.switch.ch/aai/support/documents/interfederation/>).

## ■ 2. Descriptive Information

- Update/Revise IP ranges and Domain Hints (used for IdP discovery)

## ■ 5. Contacts

- Please ensure only non-personal email addresses are listed. Ideally also add helpdesk phone numbers.

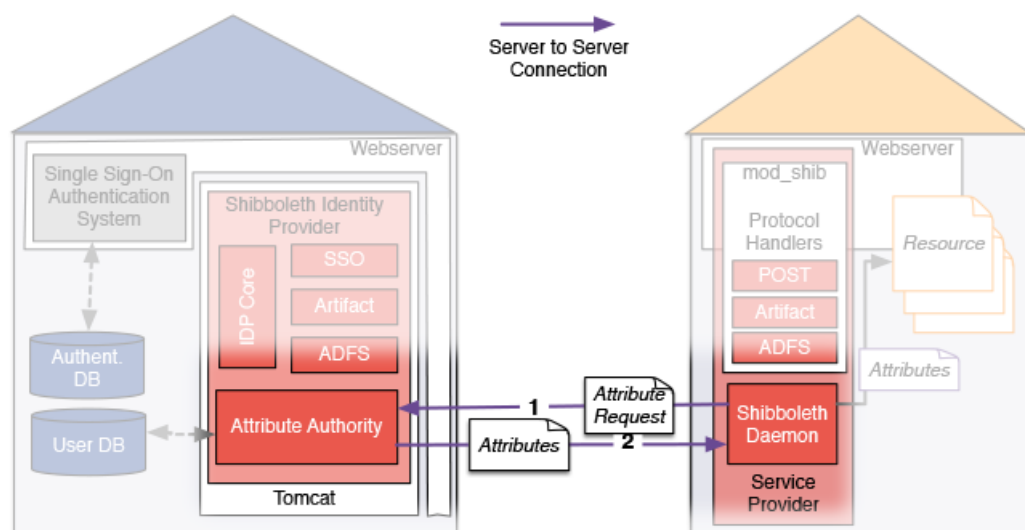
## ■ 7. Attribute Release Settings

- Default attribute release policies. Consider to release all R&S attributes!

# 2. Change URL for Attribute Authority

**Recommendation for IdPv2 has been so far:**

Separate port (i.e. 8443) or IP for IdP Attribute Authority (AA)



## 2. Change URL for Attribute Authority

### **New Recommendation for IdP:**

Use same IP and same Port (443) for Attribute Authority (AA).

### **Why?**

Easier configuration because:

- only one Apache <VirtualHost>
- one domain name and one certificate
- no X.509 client authentication needed anymore  
(SP still checks IdP webserver certificate with IdP's metadata)
- Attribute Queries are hardly used anymore  
(but will become important again for support of edu-ID)

**But how is the attribute query still  
secured without X.509 client  
authentication by the Service  
Provider?**

**SP signs attribute query request with  
his private key (message signing),  
the IdP checks signature with SP's  
public key in metadata.**

## 2. Change URL for Attribute Authority

### What to adapt in Resource Registry then?

In "3. Technical Information" change the URLs for:

- "Attribute Service"
- "Artifact Resolution Service"

Make sure they point to the URL configured during the Identity Provider deployment. Typically the **URLs change from** e.g.:

`https://aai-login.example.org:8443/idp/...` or `https://aai-aa.example.org/idp/...`  
to  
`https://aai-login.example.org/idp/...`

## 3. Remove Unnecessary Endpoints

### Which endpoints to remove?

Generally it's better to only have published in metadata what is needed and used.

So, in "3. Technical Information" consider removing end points that are hardly used.

### Candidates to remove:

- "Single Sign On Service" with "SAML2 HTTP POST SimpleSign" binding
- "Artifact Resolution Service" with "SAML1 SOAP" binding
- "Attribute Service" with "SAML1 SOAP" binding

But only remove them after verifying they are not used ...

### 3. Remove Unnecessary Endpoints

#### How to check if a profile and binding can be removed?

Check if it has been used within last few months.

If not, remove it from Resource Registry.

#### How to check if it has been used?

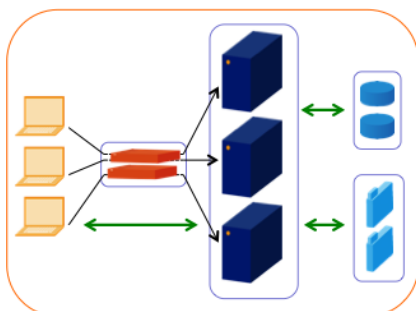
Check log files. To find if SAML1 SOAP binding logins in 2015:

```
$ cd /opt/shibboleth-idp/logs/  
$ grep 'urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding' \  
  idp-process-2015-*.log
```

Returns information (i.e. time, SP) when binding was used the last time.

## IdP Clustering

High Availability and Load Balancing



# SWITCH

SWITCHaai Team  
[aai@switch.ch](mailto:aai@switch.ch)

# You want to prevent service outages

Possible problems:

- HW failures
  - Server component failure
  - power failure.
  - Network failure
- Software failures
- Service overload
- Downtimes due to maintenance (major upgrades)
- ...

## What you usually do

- Take one box
  - Harden it through redundant components (power, network, disk, memory, CPU's, backplane (??))
- Or take another box
  - Organize failover (cold standby)
- Or take a couple of boxes
  - Organize load balancing
- ...

## Challenges with the IdP

- The setup of the IdP and the whole environment is more complex than with a single-server IdP.
- Special configuration of the IdP is required.
- Load balancing requires special hardware or software.
- IdPs in SWITCHaai store some data in a database. Therefore, clustered IdPs need some kind of clustered database or some replication mechanism.

## Stateful or not?

For stateless systems, building a cluster "is easy".  
But: The IdP is stateful, in general.

- *Conversational state*: Short-term session during login process
  - Managed outside of the IdP software
  - Requires sticky sessions on load balancer
  - At present, there is no solution provided to replicate this data
- *Non-conversational state*: Data the IdP stores
  - Managed by the IdP software
  - Examples: Persistent ID, User consent data, IdP User Session
  - The IdPv3 provides flexible mechanisms to store such data, e.g. in the client or in a common database, so that the data is available to all nodes.

## Storage Recommendations

| Storage Entity       | Recommended Storage    | Scope             |
|----------------------|------------------------|-------------------|
| Persistent ID        | <b>Common Database</b> | <b>Cluster</b>    |
| User consent         | <b>Common Database</b> | <b>Cluster</b>    |
| IdP User Session     | <b>Client</b>          | <b>Per Client</b> |
| Transient ID         | <i>Common Database</i> | Cluster           |
| SAML artifact        | <i>Common Database</i> | Cluster           |
| Conversation Session | Memory                 | Per Node          |
| Message replay cache | Memory                 | Per Node          |

Remarks:

- "Common Database" means some central/clustered database or a database replicated between nodes.
- SAML artifact:  
Irrelevant if SAML 2.0 artifacts are not used/required at all
- Alternatives for Message replay cache:  
Common Database or memcached (depending on security requirements)

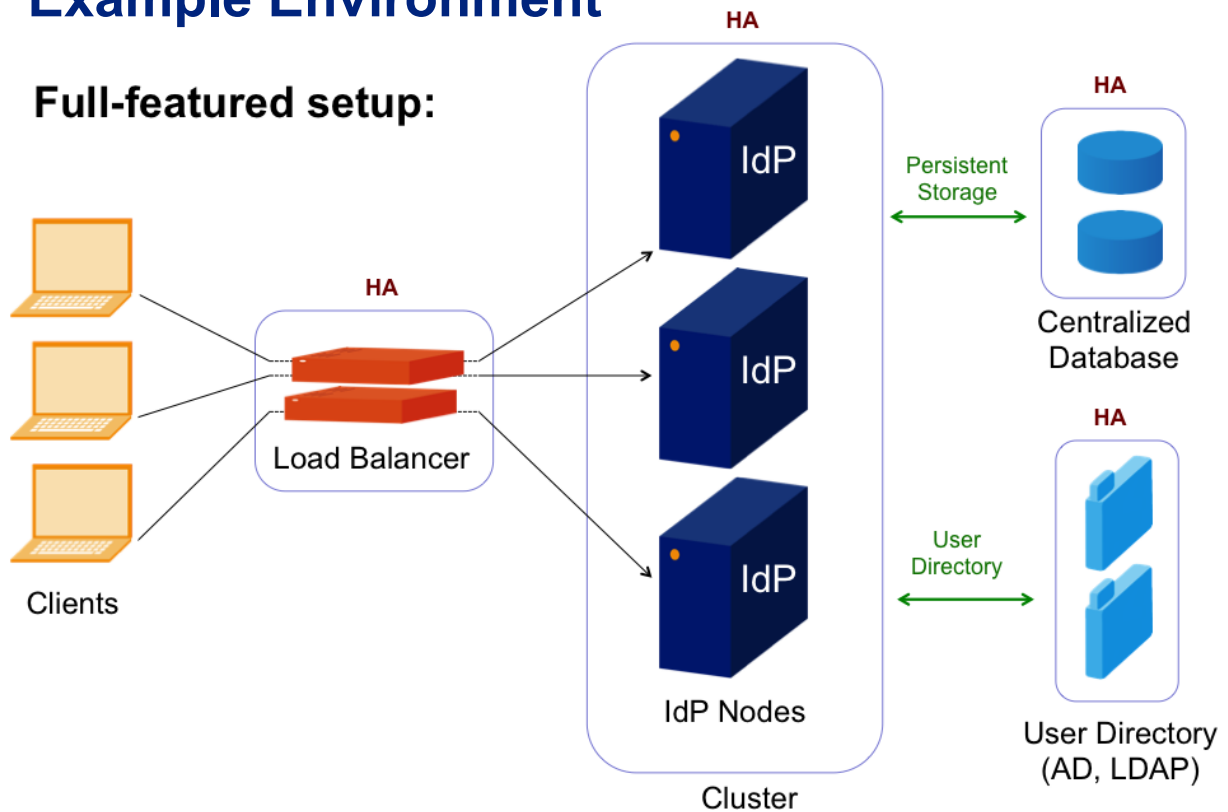
## Examples

| Who                  | Network                                    | Processing                 | Persistent storage                               |
|----------------------|--|----------------------------|--|
| Uni Bern (IdPv3)     | NGINX (active-active)<br>HTTP Loadbalancer | 2 IdPs                     | Use of central MSSQL-cluster                     |
| Uni Genève (IdPv2)   | F5 BIG-IP<br>Loadbalancer (sticky)         |                            | MySQL DB Cluster                                 |
| Uni Lausanne (IdPv2) | HW load balancer<br>(active-passive)       | 2 IdPs<br>(active-passive) | external MySQL-DB<br>(also HA: Heartbeat + DRBD) |
| Uni Zürich (IdPv2)   |  | 3 IdPs                     | external MySQL database                          |
| HES-SO Fr (IdPv2)    |  | 2 IdPs active-active       |  |
| Uni Marburg (IdPv2)  | NGINX Loadbalancer                         | 2 IdPs,<br>memcached,      | 1 external PostgresDB server                     |
| SWITCH (IdPv2)       | Anycast address                            | 2 IdPs active-passive      | Local MySQL-DB,<br>replicated by cron            |



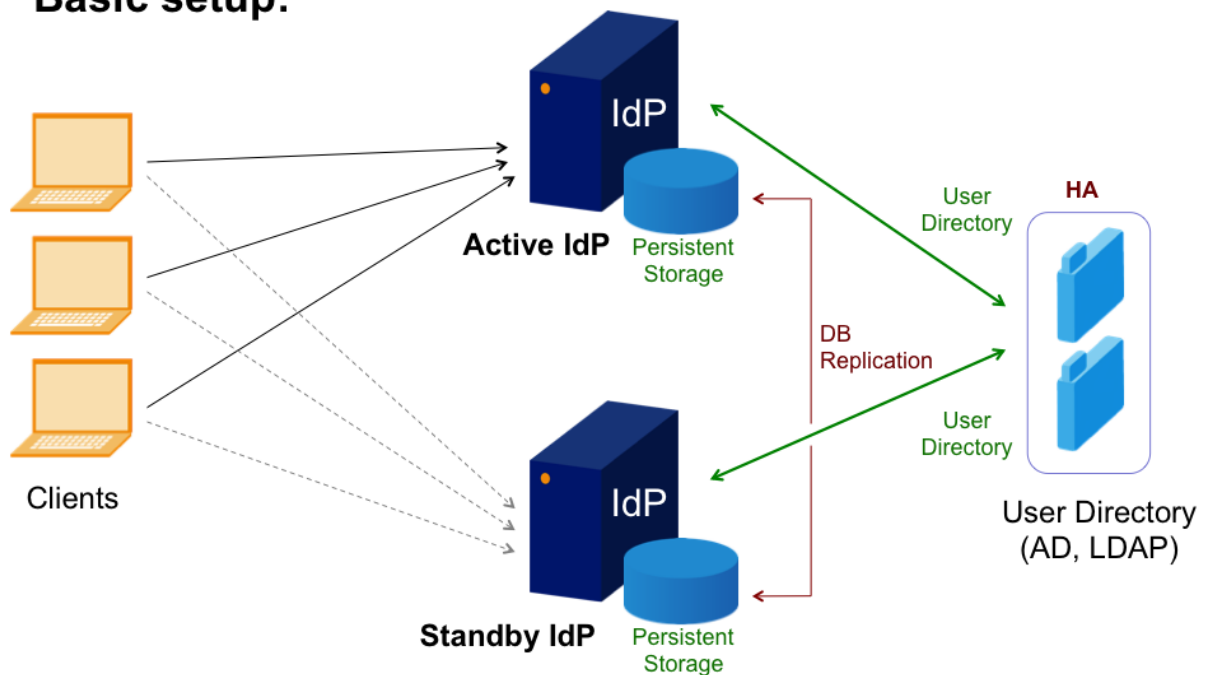
## Example Environment

### Full-featured setup:



## Example Environment

### Basic setup:



# Considerations for planning an IdP cluster

You need to think about

- Which type of setup do you need?
- What kind of database do you need?
- Which additional hardware or software is required?
- Which further considerations are relevant for your organisation?

*There are many mechanisms and options available to setup a suitable environment. The setup to choose depends on the requirements and the possibilities of your organisation.*

## References

*Documentation from SWITCH:*

- **Shibboleth IdP Clustering**  
<https://www.switch.ch/aai/guides/idp/clustering/>

*Documentation from the Shibboleth Consortium:*

- **Clustering**  
<https://wiki.shibboleth.net/confluence/display/IDP30/Clustering>
- **Storage**  
<https://wiki.shibboleth.net/confluence/display/IDP30/Storage>
- **Secret Key Management**  
<https://wiki.shibboleth.net/confluence/display/IDP30/SecretKeyManagement>

# Resource Registry Interfederation Options

Interfederation via eduGAIN and Entity Categories



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Goals

- Get an idea of the benefits when participating in interfederation
- Know what it takes to enable an IdP for Interfederation
- Understand the concept of Entity Categories
- Recognize how Entity Categories can help in a data protection conformant attribute release that scales

# Interfederation Option

What to consider before enabling an IdP for Interfederation



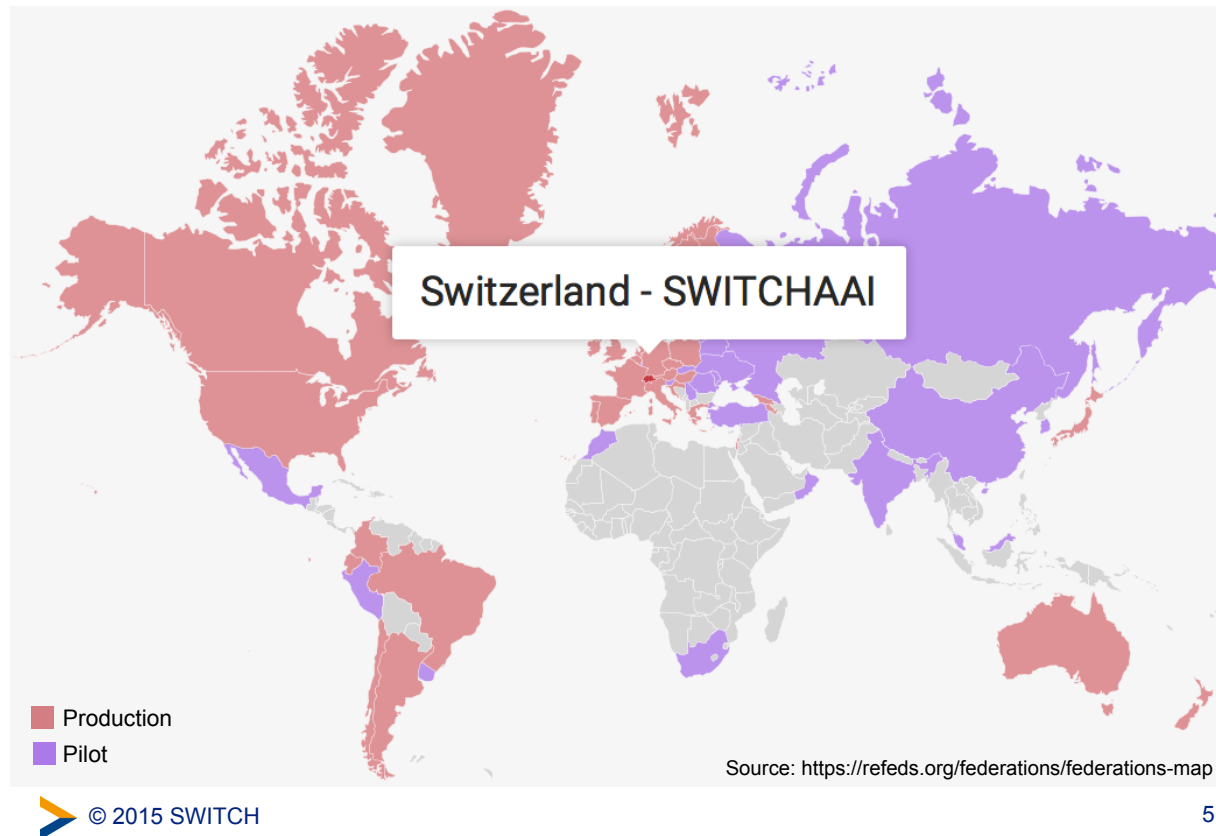
# SWITCH

SWITCHaai Team  
aai@switch.ch

## Why Interfederation?

- Most Federations are of national scope
    - Services may need to register in many federations to serve all their users. That's time consuming and becomes a huge overhead.  
e.g. EBSCOhost is registered in 22 federations!
  - Research projects are mostly multi-national
  - **Interconnecting national federations → Interfederation**
- Register the IdP or SP in only one federation and enable it for interfederation
- Enable the IdP for interfederation
    - Its users will be able to **access services from other federations**
  - Enable the SP for interfederation
    - The service can **serve users from other federations**

# All Academic Identity Federations Globally



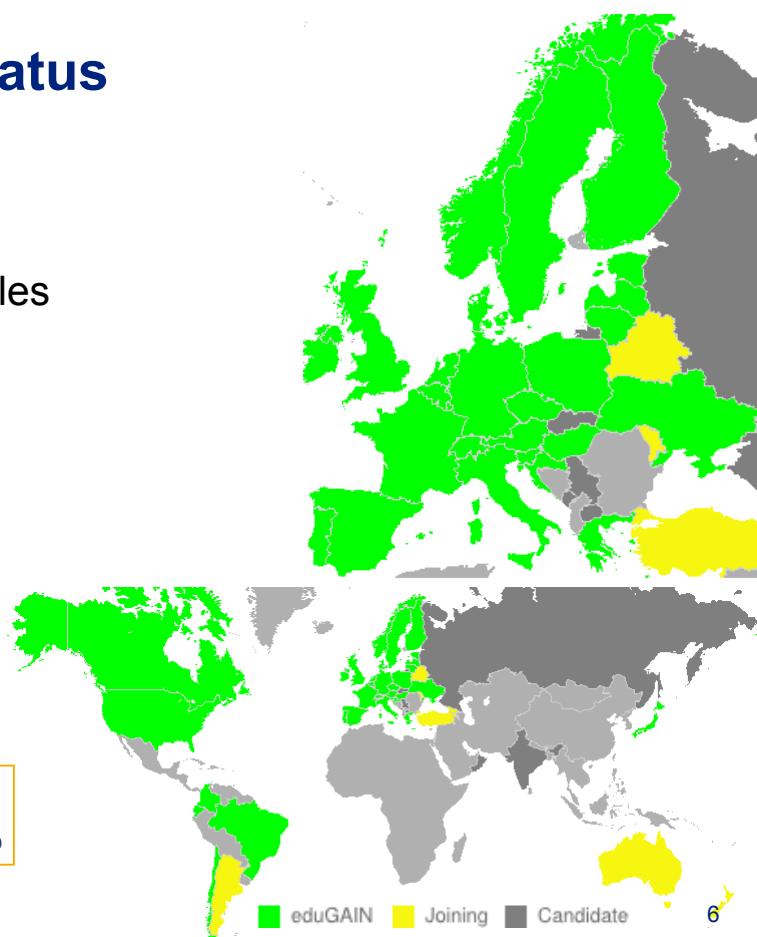
5

## Interfederation Status

- eduGAIN is the GÉANT Interfederation Service
- eduGAIN design principles
  - Low barrier to entry
  - No requirements to change local standards/procedures
  - Minimal central infrastructure
- Status August 2015
  - Total: 1412 IdPs, 965 SPs
  - From SWITCHaai: 20 IdPs, 8 SPs

<http://www.edugain.org>  
<https://technical.edugain.org/status.php>

© 2015 SWITCH



6

# Enabling Interfederation in the Resource Registry

## Prerequisite

Due to **data protection** considerations, each institution needs to sign the *SWITCHaai Interfederation Access Declaration*

→ SWITCH will enable the checkbox in the Resource Registry

| Interfederation  |   |
|--|---|
| <b>Interfederation</b>   | <input checked="" type="checkbox"/> Enable interfederation for this Home Organisation<br>Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources. |
| Enabling interfederation means that metadata about this resource is published in non-SWITCHaai organization and can be used by other Identity Providers which are not part of SWITCHaai. The metadata will also include contact information about this resource. Before enabling a service for interfederation, make sure that:  |   |
| <ul style="list-style-type: none"><li>• All internationally standardized core attributes are <u>declared as supported</u></li><li>• The default <u>attribute release policy is adapted</u> such that internationally used attributes are released to interfederation resources</li><li>• The <u>specific attribute release</u> rules are accurate and up-to-date</li></ul> |   |

<https://www.switch.ch/aai/interfederation>

## Recommended Interfederation Attributes

| Friendly name                                      | Defined in | Example  |
|--|------------|--|
| displayName  | eduPerson  | Peter Sample   |
| common name (cn)                                   | eduPerson  | Peter Sample   |
| mail   | eduPerson  | peter.sample@example.org   |
| eduPersonAffiliation<br>eduPersonScopedAffiliation | eduPerson  | staff<br>staff@example.org   |
| eduPersonPrincipalName                             | eduPerson  | 234cd8z239@example.org   |
| schacHomeOrganization                              | SCHAC      | example.org  |
| schacHomeOrganizationType                          | SCHAC      | urn:schac:homeOrganizationType:ch:university<br>urn:schac:homeOrganizationType:eu:higherEducationInstitution |
| eduPersonTargetedID /<br>Persistent Name ID        | eduPerson  | https://idp.example.org/idp/shibboleth!<br>https://sp.example.org/shibboleth!<br>2389cdhu3e-sda7323          |

eduPerson <http://www.internet2.edu/products-services/trust-identity-middleware/eduperson-eduorg/>  
SCHAC <https://wiki.refeds.org/display/STAN/SCHAC+Releases>

## Enabling Interfederation (2)

### Interfederation

#### Interfederation

☒ Enable interfederation for this Home Organisation

Activate this checkbox if users from this Home Organisation shall be able to access non-SWITCHaai resources.

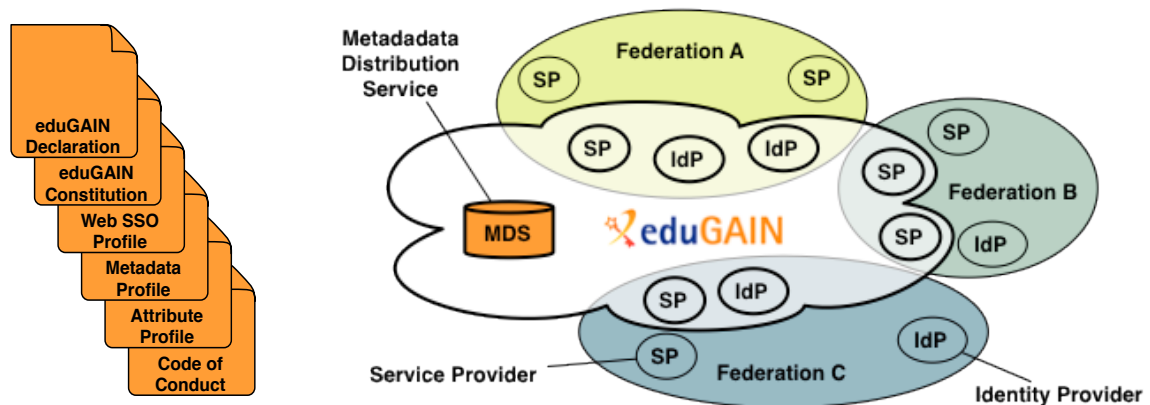
Enabling interfederation means that metadata about this resource is published in non-SWITCHaai organization and can be used by other Identity Providers which are not part of SWITCHaai. The metadata will also include contact information about this resource.

Before enabling a service for interfederation, make sure that:

- All internationally standardized core attributes are [declared as supported](#)
- The default [attribute release policy is adapted](#) such that internationally used attributes are released to interfederation resources
- The [specific attribute release](#) rules are accurate and up-to-date

<https://www.switch.ch/aai/interfederation>

## eduGAIN: What is it and how does it work? <sup>10</sup>



- eduGAIN provides policy framework and standards to build trust
- SPs and IdPs of participating federations should opt-in for eduGAIN.
  - Some federations decided for opt-out instead
- MDS fetches, aggregates and republishes metadata



# Entity Categories

GÉANT Data Protection CoCo and REFEDS Research & Scholarship R&S



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Outline

- Entity category
- GÉANT Data Protection Code of Conduct (CoCo)
- REFEDS Research & Scholarship (R&S)



## Entity categories

A generic method to enrich metadata

- Tag an entity (SP or IdP) as being part of a category
- Requires a specification for international coherent use
  - Criteria
    - Purpose
    - Policies
    - Or other

In interfederation context:

- Filling the gap of missing common policies
- Support or increase scalable trust

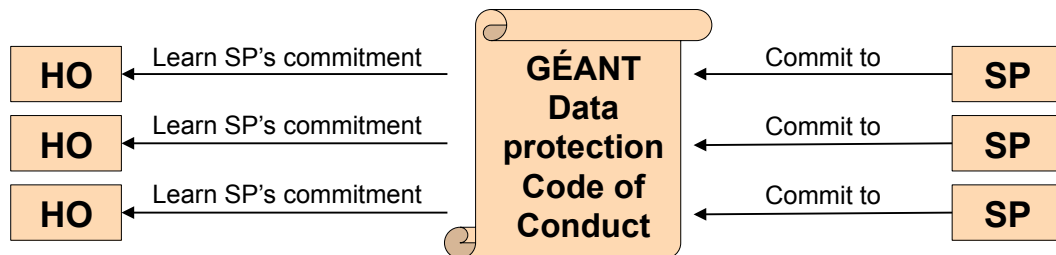
## Metadaten

```
<!-- AAI Viewer Interfederation Test -->
<EntityDescriptor entityID="https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth">
  <Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        Name="http://macedir.org/entity-category"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1
        </saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        FriendlyName="swissEduPersonHomeOrganization" Name="urn:oid:2.16.756.1.2.5.1.1.4"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>switch.ch</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        FriendlyName="swissEduPersonHomeOrganizationType" Name="urn:oid:2.16.756.1.2.5.1.1.5"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>others</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </Extensions>
  ...
</EntityDescriptor>
```

## GÉANT Data Protection Code of Conduct

### Increase the trust in Service Providers (SPs)

- The method is based on the EU Data Protection directives
- The SP has to provide a Privacy Policy (in English, according to the guideline)
- That will encourage the Home Organisation IdP to release attributes
  - ➔ attribute release will scale



### Code of Conduct Toolkit

- **Data Protection Code of Conduct for SPs in EU/EEA**
- Entity category attribute definition for the Code of Conduct
- SAML2 profile for the Data Protection Code of Conduct

## GÉANT Data Protection Code of Conduct

- **Principles:**
  - Legal compliance
  - Purpose limitation
  - Data minimisation
    - Deviating purposes
    - Data retention
    - Third parties
    - Security measures
  - Information duty towards end user
  - Information duty towards home organization
  - Security breaches
  - Liability
  - Transfer to third countries
  - Governing law and jurisdiction
  - Eligibility to execute
  - Termination of the Code of Conduct
  - Survival of the clauses
  - Precedence

# Data Protection Code of Conduct (DP CoCo)

## Normative documents

- [Data Protection Code of Conduct for SPs in EU/EEA](#)
- Entity category specification for the DP CoCo
- SAML2 profile for the DP CoCo

<http://www.geant.net/uri/dataprotection-code-of-conduct/v1/>

## Non-normative, informational documents

- Introduction
- Introduction to the DP directive
- Managing DP risks using CoCo
- [Privacy policy guidelines for SPs](#)
- What attributes can an SP request
- [DP good practice for Home Organisations](#)
- Federation operator guidelines
- Handling non-compliance
- [IdP inform/consent GUI guidelines](#)

<https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home>

## Cookbook for DP CoCo

[https://wiki.edugain.org/Data\\_Protection\\_Code\\_of\\_Conduct\\_Cookbook](https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook)

# Privacy policy template

- Name of the service
- Description of the service
- Data controller and a contact person
- Jurisdiction
- Personal data processed
- Purpose of the processing of personal data
- Third parties to whom personal data is disclosed
- How to access, rectify and delete the personal data
- Data retention
- Data Protection Code of Conduct

## REFEDS Research & Scholarship

- R&S SPs support
  - Research & scholarship interaction
  - Collaboration
  - Management
- No SPs from publishers!
- Attributes:
  - Personal identifiers: email, person name, eduPersonPrincipalName
  - Pseudonymous identifier: eduPersonTargetedID
  - Affiliation: eduPersonScopedAffiliation
- Minimal subset: eduPersonPrincipalName, mail, person name

(person name = given name + surname OR displayName)

## Comparison

| REFEDS R&S                | GÉANT DP CoCo                    |
|---------------------------|----------------------------------|
| Global                    | Mainly Europe                    |
| Common purpose of the SPs | Common data protection standards |
| Fixed set of attributes   | SP can require any attributes    |

# Attribute Release Configuration

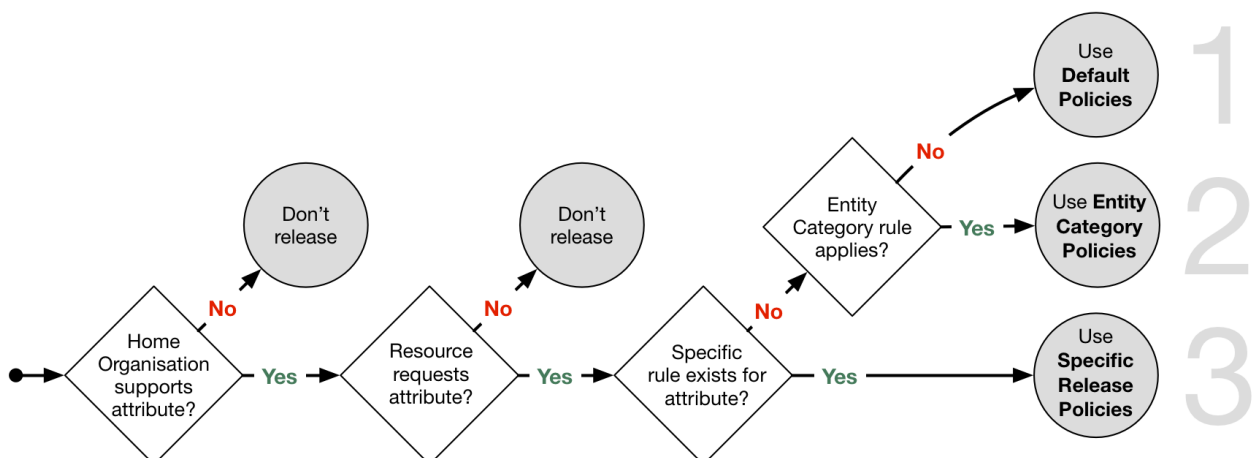
How attributes are released



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Attribute Release Rules



# Attribute Release Settings (1)

Resource Registry –  
Edit Home Organization Description –  
Attribute Release Settings

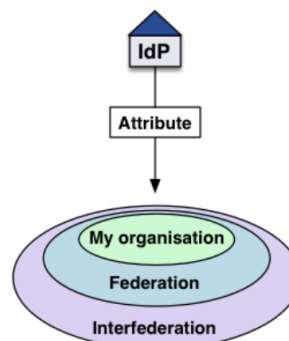
## 1. Default Policies for Individual Attributes

Individual default Attribute Release Policy rules apply if no Resource Specific Attribute Release Policy rule exists and if the Service Provider is not in one of the above Entity Categories. Only [supported attributes](#) are listed below.

### Release Scopes

The release policy rules for individual attributes allow to set one of the following release scopes to which to release an attribute by default. Release attribute to:

- **Nobody**: The attribute is never released except if there is a Resource Specific Attribute Release Policy rule, which overrides all other rules.
- Resources of **My organization** (SWITCH): The attribute is released only to [resources of SWITCH](#), excluding Federation Partner resources.
- Resources in the (SWITCHaai) **Federation**: The attribute is released to all [SWITCHaai resources](#).
- **Interfederation** (e.g. [eduGAIN](#)) resources: The attribute is released to all [interfederation resources](#) as well as to all Resources from the enclosed release scopes. The following attributes are recommended to be released to Interfederation resources if they are required:
  - Principal Name (unique identifier)
  - Targeted ID (unique identifier)
  - Affiliation (e.g. staff, student, faculty, affiliate)
  - Scoped affiliation (same as affiliation but domain name appended)
  - E-Mail
  - Display Name (full name)
  - Common Name (same as display name but can be multi-valued)
  - SCHAC Home Organisation (like Swiss Home Organization)
  - SCHAC Home Organisation Type (similar like Swiss Home Organization Type)



Release ...      ... required attributes to      ... desired attributes to

Have a look at the diagram above in order to understand the effects of the different policy choices below.

### SWITCHaai Attributes

Affiliation ([core](#))

interfederation resources

SWITCHaai resources



© 2015 SWITCH

3

# Attribute Release Settings (2)

## 2. Entity Category Policies

Entity Category Policies apply whenever a Resource claims to meet the category's requirements. The claim is part of the Service Provider's metadata. Entity Category Policies have higher priority than the default release policies for individual attributes. However, they have lower priority than the Resource Specific Attribute Release Policy rules.

Together with a user attribute release consent module (i.e. [uApprove](#)), attribute release based on the entity categories below should provide enough confidence from a data protection point of view to release the requested attributes also to Interfederation-enabled resources abroad.

### GÉANT Data Protection Code of Conduct (CoCo)

Resources in the [GÉANT Data Protection Code of Conduct \(CoCo\)](#) entity category declare to respect the CoCo's behavioral rules and that they are located in either EU/EEA or a country with adequate data protection (e.g. Switzerland).

The CoCo was created by [GÉANT](#), the international research infrastructure project that also created and operates [eduGAIN](#) and [eduroam](#). SWITCH contributes to GÉANT.

Release required attributes (default)

Provided a Resource is in the GÉANT Data Protection Code of Conduct entity category and attribute release for this entity category is enabled, an attribute is only released if its release scope is neither **nobody** nor **my organisation's resources**. Is the attribute release for this entity category disabled, only the default and specific release rules apply.

### REFEDS Research & Scholarship (R&S)

Resources in the [REFEDS Research & Scholarship \(R&S\)](#) category "enhance the research and scholarship activities" and are of benefit to R&S user communities.

[REFEDS](#) specified this entity category. It is the interest group of research and education identity federations world-wide. SWITCH contributes to REFEDS.

Release minimal set of R&S attributes (default)

The minimal R&S attribute set includes the attributes:

- **Principal name**
- **E-mail**
- **Name (Given name and surname or alternatively Display name)**

The complete set with all R&S attributes additionally includes:

- **Targeted ID/Persistent ID**
- **Scoped Affiliation**

Is the attribute release for this entity category disabled, only the default and specific release rules apply.

## 3. Resource Specific Policies

Resource Specific Attribute Release Policy rules have always precedence over all other attribute release policies.

Set or review the specific rules: [Resource Specific Attribute Release Policy rules](#).

4

# IdP Overview of Log Files



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Apache log files

- `access.log`
  - `aai-login.example.org.access.log`
- `error.log`
  - `aai-login.example.org.error.log`
  - LogLevel in `/etc/apache2/apache2.conf` (default “warn”)

Location: `/var/log/apache2`

Configuration defined in the virtual host definition

- Directory: `/etc/apache2/sites-available/`
- File: `aai-login.example.org.conf`

## Tomcat log files

- `catalina.out`
  - Console output (`System.err/out`) from Tomcat
  - Default location: `/var/log/tomcat7/`
  - Configured in `/etc/tomcat7/logging.properties`
- `{catalina,localhost}.YYYY-MM-DD.log`
  - Same as `catalina.out`
- `localhost_access_log.YYYY-MM-DD.txt`
  - Access information associated with a request: IP address, time, request method (GET or POST)
  - Default location: `/var/log/tomcat7/`
  - Configured in `/etc/tomcat7/server.xml`

## Shibboleth log files (1)

- Logging framework called “Logback”
- Implementation of SLF4J
- Manual:
  - <http://logback.qos.ch/manual/index.html>
- On-the-fly configuration reloading
  - Change log level without restarting the IdP
  - Reload interval set in `services.properties`
    - entry `idp.service.logging.checkInterval = PT5M`
- Option: send email alerts



## Shibboleth log files (2)

- Location: `/opt/shibboleth-idp/logs`
- Four log files produced by default
  - `idp-process.log`: detailed description of the IdP processing requests
  - `idp-warn.log`: only warnings and errors
  - `idp-audit.log`: attribute release auditing records
  - `idp-consent-audit.log`: user decisions over attribute release and terms of use acceptance
- Daily rollover with compression, 6 months history

## Shibboleth log files (3)

Configured in `/opt/shibboleth-idp/conf/logback.xml`

- 3 main classes: Logger, Appender (output destination) and Layout
- Default settings usually OK
- Example changes
  - LDAP Auth. Module or authentication events
  - new Logger or Appender...
- Log messages have 5 levels: TRACE, DEBUG, INFO, WARN, ERROR

# SMTPAppender in logback.xml

```
<appender name="EMAIL"
  class="ch.qos.logback.classic.net.SMTPAppender">
  <smtpHost>localhost</smtpHost>
  <to>staff1@example.org</to>
  <from>idp_host@example.org</from>
  <subject>TESTING: %logger{20} - %m</subject>
  <layout class="ch.qos.logback.classic.PatternLayout">
    <pattern>%date %-5level %logger{35} - %message%n</pattern>
  </layout>
</appender>

<root level="DEBUG">
  <appender-ref ref="IDP_PROCESS"/>
  <appender-ref ref="IDP_WARN" />
  <appender-ref ref="EMAIL" />
</root>
```

<http://logback.qos.ch/manual/appenders.html>



7

## Hands On 1



Why is Tomcat not starting up?

1. Edit `/etc/tomcat7/server.xml` and edit jasper listener in Server Element (wrong class!)  

```
<Listener
  className="org.apache.catalina.JasperListener
```
2. Restart Tomcat
3. Look at `/var/log/tomcat7/catalina.out`
  - Find the entry `java.lang.ClassNotFoundException`
4. Undo edit jasper listener in `server.xml` and restart Tomcat



8

## Hands On 2



- Find out why not all of the attributes appear

AAI Demo - Mozilla Firefox

SWITCH (CH) https://aai-demo.switch.ch/secure/

Most Visited > Training Page > AAI Demo > IdP Installation Guide > IdP Status

AAI Demo

SWITCH

About AAI

Area: Any authenticated user

Shibboleth Service Provider, current <RequestMap />:

```
<Path
  name="secure"
  authType="shibboleth"
  requireSession="true">
</Path>
```

| Attributes  | Values  |
|---|---|
| homeOrganization  | example.org   |
| SAML2 Attribute Name: urn:oasis:names:tc:SAML:2.0:attr:urn:oid:2.16.756.1.2.5.1.1.4 |   |
| homeOrganizationType  | others  |
| SAML2 Attribute Name: urn:oasis:names:tc:SAML:2.0:attr:urn:oid:2.16.756.1.2.5.1.1.5 |   |
| Shib-Application-ID   | default   |
| Shib-Authentication-Instant   | 2015-06-02T13:44:02.265Z  |
| Shib-Authentication-Method  | urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport |
| Shib-AuthnContext-Class   | urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport |
| Shib-Identity-Provider  | https://aai-login.example.org/idp/shibboleth                      |
| Shib-Session-ID   | 0427dc9d4e770d919578588d1e7afe75                                  |
| Shib-Session-Index  | 73fd11a815c1c7267b57b756a9fe86                                    |

## Hands On 2



1. `cd /opt/shibboleth-idp/conf/`
2. Edit `ldap.properties` and insert wrong value:  
Change entry `idp.attribute.resolver.LDAP.searchFilter` to value `(uid=$requestContext.Name)`
3. Edit `logback.xml`:
  - Set log level to `DEBUG` for logger `org.ldaptive.auth.Authenticator`
  - Insert additional logger for the attribute resolver:  

```
<logger name="net.shibboleth.idp.attribute.resolver" level="DEBUG" />
```
4. Restart Tomcat and log in to the IdP (AAI Demo Service)
5. Look at the `idp-process.log` and find the log entries:  

```
[org.ldaptive.auth.Authenticator:284]
[net.shibboleth.idp.attribute.resolver.dc.ldap.impl.Template...:203]
```
6. Undo wrong value: set `$requestContext.principalName` and restart Tomcat

# IdP Reloading the Configuration

New options with IdPv3



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Reloading the configuration with v2

- only supported in a limited way – by setting the `configurationResourcePollingFrequency` attribute of one these services to a short value:
  - attribute resolver (`attribute-resolver.xml`)
  - attribute filtering engine (`attribute-filter.xml`)
  - profile handler manager (`handler.xml`)
  - relying party configuration manager (`relying-party.xml`)
- potentially dangerous when repeated reload attempts fail (by default, `configurationResourcePollingRetryAttempts` is only set to 3, after which reloading stops)
- no option to explicitly trigger a reload, so only achieved by a relatively awkward constantly-watch-for-file-changes check

## New reloading options with v3

- reload is explicitly triggered by calling two special-purpose **admin flows**, which are configured under  
`https://aai-login.example.org/idp/profile/admin/reload-service?id=bean-id`  
`https://aai-login.example.org/idp/profile/admin/reload-metadata?id=md-id`
- available bean IDs for service reloads: see  
`$ grep "bean id=.*class" /opt/shibboleth-idp/system/conf/services-system.xml`  
and the corresponding resource lists in **services.xml**
- reloading metadata: find the IDs with  
`$ grep Provider.*id /opt/shibboleth-idp/conf/metadata-provider-*.xml`
- by default, access to the `reload-*` URLs is restricted to localhost (and if `access-control.xml` is configured as suggested in the SWITCH installation guide, to the AAI Resource Registry)
- two reload scripts get installed under `/opt/shibboleth-idp/bin`, and serve the same purpose  
depend on **JAVA\_HOME** being set, and a proper `-u` argument being specified...  
requesting the respective URL with `curl` seems more straightforward

## Available bean IDs for service reloads

**shibboleth.LoggingService**: logging configuration reload (`logback.xml`)  
**shibboleth.AttributeFilterService**: attribute filter reload  
**shibboleth.AttributeResolverService**: reloads attribute and data connector definitions (`attribute-resolver-*.xml` files)  
**shibboleth.NameIdentifierGenerationService**: reloads the configuration in the `saml-nameid.xml` file  
**shibboleth.RelyingPartyResolverService**: reloads `relying-party.xml` and `credentials.xml`  
**shibboleth.MetadataResolverService**: reloads the metadata list specified in `services.xml`  
**shibboleth.ReloadableAccessControlService**: reloads the configuration in the `access-control.xml` file

Missing from this list: an ID for reloading the **shibboleth.MessageSourceResources** list, i.e. the message text files under `/opt/shibboleth-idp/messages/`.  
By default, the IdP only caches these for five minutes, however, so they are reloaded automatically (see also `idp.message.cacheSeconds` in `services.properties`).

## And restartless login page editing, too

- the IdP v3 has switched to Velocity templates as the new default mechanism for rendering the login (and error) pages
  - edit the `.vm` files under `/opt/shibboleth-idp/views/`, and the changes become effective immediately
  - say goodbye to container restarts (Tomcat), which was required when JSP files were changed with the IdP v2

## Still requiring a restart with v3

- changes to the contents of `services.xml`  
i.e., changes to the `<util:list>` elements themselves (such as adding an additional `attribute-resolver-*.xml` file)
- changes to `global.xml` (SQL data source, HTTP client settings)
- changes to the authentication configuration, such as LDAP parameters etc.
- changes to `/opt/shibboleth-idp/edit-webapp/...` files  
(need `build.sh` to be run first, followed by a container restart)
- and a few more, of course... but under normal operating conditions, such reconfigurations relatively rarely occur



## (Ideas for) hands-on exercises

- try reloading a couple of the services listed on slide 4  
`curl https://aai-login.example.org/idp/profile/admin/reload-service?id=...`
- check what happens when specifying invalid bean IDs
- insert a syntax error into a configuration file, and try reloading the corresponding service
- entries in `idp-audit.log` just record reload events with  
...|||||http://shibboleth.net/ns/profiles/reload-metadata|||||||  
...|||||http://shibboleth.net/ns/profiles/reload-service-configuration|||||||  
How can you determine what `id=` argument was supplied?
- what is an easy method to quickly print the currently running IdP and Java version details to `idp-process.log`?

## New Challenges with Interfederation SPs?

Interfederation unites various cultures



# SWITCH

SWITCHaai Team  
aai@switch.ch

## Goals

- Get an idea of why access to an interfederated SP might fail differently than in SWITCHaai
- Understand what is different regarding
  - Opt-in vs. opt-out
  - Metadata
  - Discovery Service
  - Attributes
- Know whom to contact and where to get help

## Interfederation Rollout: Opt-in vs. Opt-out

- Opt-in
  - IdPs and SPs decide when they are ready to interfederate
    - Once the configuration is up-to-date
      - Interfederation Metadata gets loaded
      - IdP: Additional attributes, user consent
      - SP: Discovery Service, attribute mapping, access rules
  - ⊖ Slow process
  - ⊕ Entities unlikely to cause interoperability problems
- Opt-out
  - Federation announces a flag day for enabling interfederation
    - IdPs and SPs need to opt-out before
      - if they do not want to participate
      - if they are not yet ready
  - ⊕ Quick adoption
  - ⊖ More likely that entities cause problems, unless they opted-out before the flag day





## Three Examples

- 1) UK Data Archive  
<http://www.data-archive.ac.uk>
- 2) FUNET FileSender  
<https://filesender.funet.fi>
- 3) WISEflow  
<https://europe.wiseflow.net>

What is wrong in these examples?

- 1) Unclear use of terminology at the SP to know whether interfederation is supported or not  
Central discovery service of the UK Federation lists all interfederated IdPs, even when the service did opt-out
- 2) eduGAIN shown as an option, but no IdPs available that are interfederated via eduGAIN
- 3) eduGAIN is not available as an option to pick from, despite the SP is published to eduGAIN

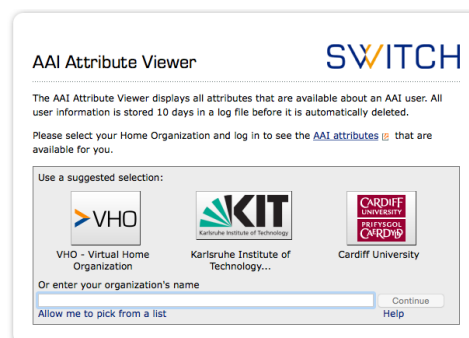
## Metadata

<meta><data>

- Interfederated IdPs and SPs need additional metadata
  - SWITCHaai entities configure an additional metadata source signed with the same trust anchor.
  - 'Opt-out federations' integrate all entities into a single metadata file.
- Propagation speed of metadata changes
  - In SWITCHaai: two hours
  - For interfederation: one to a few days
- Possible issue
  - SP does not load interfederation metadata
    - SP does not know the IdP and fails.

## Discovery Service (DS)

- Within SWITCHaai, users easily find their IdP
- An SP needs a DS that knows the appropriate set of IdPs
  - An interederation enabled SP registered in SWITCHaai needs to deploy a DS that includes interederation
  - E.g. in the UK Federation the central DS lists always all interfederated IdPs, also for SPs that did opt-out
  - That can result in such an error message at your IdP:  
**Shibboleth SSO profile is not configured for relying party <https://sp.example.org/shibboleth-sp>**



## Attributes

- Missing attributes cause interoperation problems
  - Check SP's attribute requirements in the Resource Registry
  - Verify that attributes were released (in IdP's `audit.log`)
    - If NO: check your IdP's attribute release policy
    - If YES
      - Were all required attributes released?
        - If YES: SP has to check it out why it fails
        - If NO: review your attribute release policy
- Another issue:
  - An SP failed because it was not able to decrypt the SAML assertion that included the attribute values.  
The SP's federation used only signed but not encrypted SAML assertions, so that problem was not discovered earlier

## Exploring interfederated entities

- Is a university's IdP or an SP already interfederated?
  - go to: <https://technical.edugain.org/status.php>
  - pick the country where the entity might be registered
  - under 'Metadata URL' click on 'validate this metadata set', then on 'show entities list'
- or search it in the **eduGAIN List of Entities**
  - go to: <https://technical.edugain.org/entities.php>
- or try the **Is Federated Checker**
  - go to: <https://wiki.edugain.org/isFederatedCheck/>
  - provide email addresses or domain names
- Additional web pages of interest
  - Which interfederated SPs are committed to the GEANT Data Protection Code of Conduct (CoCo)?
    - go to: <http://monitor.edugain.org/coco/>
  - **REFEDS Metadata Explorer Tool (MET)**
    - go to: <https://met.refeds.org/>

## Troubleshooting interfederated entities

- Find an SP in the Resource Registry
  - go to: <https://rr.aa.switch.ch/>
  - pick 'Search for resources'
  - pick 'interfederation'
- or search it in the metadata file 😊
  - `/opt/shibboleth-idp/metadata/metadata.interfederation-sps.xml`
- Contact the SWITCHaai Team  
➔ `aai@switch.ch`

• 🔍 [Search for resources:](#) !

Interfederation